

T.R.
ISTANBUL MEDENIYET UNIVERSITY
INSTITUTE OF GRADUATE EDUCATION
DISCIPLINE OF PRIVATE LAW

**CIVIL LIABILITY OF DATA CONTROLLER FOR UNLAWFUL
PROCESSING OF PERSONAL DATA**

MASTER'S THESIS

MURAT UÇAK

JUNE 2019

T.R.
ISTANBUL MEDENİYET UNIVERSITY
INSTITUTE OF GRADUATE EDUCATION
DISCIPLINE OF PRIVATE LAW

**CIVIL LIABILITY OF DATA CONTROLLER FOR UNLAWFUL
PROCESSING OF PERSONAL DATA**

MASTER'S THESIS

MURAT UÇAK

THESIS SUPERVISOR
PROF.DR. ÜMİT GEZDER

JUNE 2019

DECLARATION

I hereby declare that this thesis prepared by me is completely my own work, that I prepared it by observing the academic rules and ethical conduct and that all the quotations cited are referenced.


Signature

Murat Uçak



I hereby declare that this thesis, for which I am the supervisor, is fully the work of my student, that he worked by observing the academic rules and ethical conduct.

Prof. Dr. Ümit Gezder



APPROVAL PAGE

This master's thesis prepared by Murat Ucak with the
title Civil Liability of Data Controller For Unlawful Processing Personal
Data is prepared at the Discipline of
Private Law and is accepted by our jury.

JURY MEMBERS

Thesis Supervisor:

[PROF. DR, ÜMİT GEZDER]

Institution: İstanbul Medeniyet University

Members:

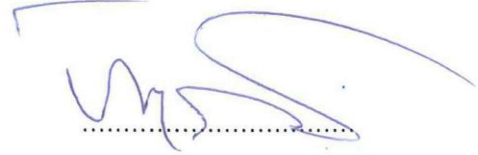
[PROF. DR, M. REFİK KORKUSUZ]

Institution: İstanbul Medeniyet University

[PROF. DR, EMREHAN İNAL]

Institution: İstanbul University

SIGNATURE



Thesis Defense Date: 13 / 06 /2019

PREFACE

With the effect of the modern world and developing technology, people are to faced with different and new legal problems, which leads to the formation of new branches of law or to update of existing branches of law. The personal data protection concept, which is the main subject of this study, is an important issue since the first period of history. In this day and age, however, this concept has become more an important issue because the fact that personal data can be collected, obtained, transferred to third parties and stored or classified in much easier way may violate the fundamental rights and freedoms of individuals. Therefore, the right to protection of personal data has emerged and thus the protection of individuals is aimed.

I had the opportunity to understand the importance of protection of personal data and its relation with the law in detail for the first time thanks to the “E-Commerce” course, I took during my master course period. As a result of my research for a task given in this course, I concluded that there are many academic studies about personal data in EU and USA, but such detailed studies are lacking in our country. However, personal data is crucial issue required to be examined in a detailed way in terms of both economic and fundamental rights and freedoms. With the encouragement of my thesis advisor Prof. Dr. Ümit GEZDER, my desire to examine this issue in more detailed strengthened.

Since I will write my thesis in English, the thesis subject I would determine must have been both handled current and in a detailed way in international academic society and should have been associated with particularly civil law in Turkey. Thus, I have determined the protection of personal data issue at the heart of the discussions about both the LPPD, which has come into force in our country and the GDPR, which has entered into for in EU. In many studies in our country, the right to protection of personal data has been handled within the scope of constitutional law, criminal law or administrative law, but not much has been done study about how individuals will suffer damage in the result of unlawful processing of personal data activity and how these damages can be compensated. Thus, I decided to examine the protection of personal data within the framework of “compensation law”.

I would like to express my utmost gratitude and sincere thanks to my advisor Prof Dr. Ümit GEZDER who saw the first seeds of emergence of this study, prepared work environment to me abroad and domestic for the research despite the workload of our department, shared his experience with me about periods of thesis; our university dean Prof. Dr. M. Refik KORKUSUZ who led the establishment of the LLM program in our university, encouraged me to write my thesis despite my reservations about writing a Master’s thesis in English; Prof. Dr. Emrehan İNAL who I have been his student during my undergraduate years, participated as a guest professor in the my thesis jury.

Moreover, I would like to thank a dear colleague and friend Research Assistant M. İsmail Çekiç who helped for my works at the university when I went to Spain to do

research, provided moral support. And finally, I would like to express boundless grateful to my dear family for continuous support, motivation and, encouragement.

Murat Uçak
Üsküdar, Temmuz 2019



ÖZET

KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİNDE VERİ SORUMLUSUNUN HUKUKİ SORUMLULUĞU

Uçak, Murat

Yüksek Lisans Tezi, Özel Hukuk Anabilim Dalı

Danışman: Prof. Dr. Ümit Gezder

Haziran, 2019,189

Bu çalışmanın amacı kişisel verilerin hukuka aykırı işlenmesi sonucunda oluşacak ilgili kişinin zararlarının ne şekilde tazmin edileceğini Medeni ve Borçlar Kanunu çerçevesinde detaylıca incelemektir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesinden önce kişisel veriler kişilik haklarının korunması kapsamında genel hükümlere göre korunmaktaydı. KVKK ile hangi durumlarda kişisel verilerin işlenmesinin hukuka aykırı olacağı netlik kazanmıştır. Bu çalışmada, kişisel verilerin hukuka aykırı işlenmesi sonucunda genel sorumluluk hukuku kapsamında veri sorumlusunun ilgili kişinin zararlarını ne şekilde tazmin edeceğine cevap aranmıştır.

Bu cevaba ulaşmak için, öncelikle kişisel veri kavramı ele alınmış, koruma kapsamına hangi kişilerin gireceği ve ne kapsamda korumanın gerçekleşeceği incelenmiş ve işleminin hukuka uygun olduğu haller ele alınmıştır. Sonrasında ise, veri sorumlusu ve veri işleyen sorumluluğuna neden olan hukuki sebepler detaylıca incelenmiştir. Son olarak da bu sorumluluğun doğması sonucu ne tür zararların ne şekilde karşılanacağı tazminat davası hükümleri çerçevesinde irdelenmiştir.

Böylece veri sorumlusunun kişisel verileri hukuka aykırı işlemesi sonucu meydana gelecek özel hukuk sorumluluğu detaylı şekilde ele alınmıştır.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Veri sorumlusu, Hukuki Sorumluluk, Tazminat Davası

ABSTRACT

CIVIL LIABILITY OF DATA CONTROLLER FOR UNLAWFUL PROCESSING OF PERSONAL DATA

Uçak, Murat

Master's Thesis, Discipline of Private Law

Thesis Supervisor: Prof. Dr. Ümit Gezder

June, 2019,189

The purpose of this study is to examine, within the frame of the Civil Code and the Code of Obligations, how to remedy the damages to be suffered by the data subject as a result of unlawful processing of the personal data.

Before the Law on Protection of Personal Data No 6698 took effect, the personal data were protected within the scope of the protection of the personal rights. The cases where such personal data processing shall be unlawful are clarified by the LPPD. In this study, the answers are sought for the remedy by the data controller, of the damages suffered by the data subject as a result of unlawful processing of personal data within the frame of the general liability law.

In order to find these answers, first, the concept of personal data is focused on, the persons to be included within the scope of the protection and the extent of the protection are examined and the cases in which the processing is lawful are discussed. Afterwards, the legal reasons resulting in the liability of the data controller and the data subject are examined in detail. Finally, the types of damages to be remedied and the manner of remedy as a result of occurrence of this liability are examined within the frame of the provisions of the action of compensation.

Accordingly, the private law liability of the data controller as a result of unlawful processing of personal data is examined in detail.

Keywords: Personal Data, Protection of Personal Data, Data Controller, Civil Liability, Action for Compensation

TABLE OF CONTENTS

PREFACE	iii
ÖZET.....	iv
ABSTRACT.....	v
ABBREVIATIONS	viii
INTRODUCTION	1
1. THE SIGNIFICANCE AND OBJECTIVE OF THE SUBJECT	1
2. BOUNDARIES OF THE RESEARCH	4
3. THE PLAN OF THE RESEARCH.....	5
4. SOURCES OF THE RESEARCH	6

SECTION I

THE CONCEPTS AND FUNDAMENTAL PRINCIPLES CONCERNING THE PERSONAL DATA

1. THE CONCEPT OF PERSONAL DATA AND ITS LEGAL NATURE	9
1.1. The Concept of Personal Data.....	9
1.1.1. Information.....	11
1.1.2. Identified or Identifiable Person.....	13
1.1.2.1. Protection of the Children’s Personal Data	16
1.1.2.2. Opinions on Protection of the Personal Data of Deceased Persons	18
1.1.2.3. Protection of the Unborn Children within the scope of the	
Personal Data Protection Law	20
1.1.2.4. Distinguishing the Identified or Identifiable Person	22
1.1.3. Relating to a Person	24
1.2. Categories of Personal Data	25
1.2.1. Personal Data of Special Nature	25
1.2.2. Ordinary Personal Data	28
1.3. Legal Nature of Personal Data	29
1.3.1. Opinion of Personal Right.....	29

1.3.2.	The Opinion of Property Right	32
1.3.3.	Intellectual Property Right Opinion.....	35
2.	OTHER CONCEPTS IN THE PERSONAL DATA PROTECTION LAW... 36	
2.1.	Data Controller.....	36
2.1.1.	Legal Personality of the Data Controller	37
2.1.2.	Determination of the Purposes and Means of Data Processing	38
2.1.3.	Joint Data Controllers	40
2.2.	Data Processor.....	41
2.3.	The Concept of Processing of Personal Data.....	42
2.4.	Data Registry System.....	44
3.	FUNDAMENTAL PRINCIPLES IN DATA PROTECTION LAW.....	44
3.1.	Lawfulness and Conformity with Rules of Bona Fides	46
3.1.1.	Lawfulness	46
3.1.2.	Conformity with Rules of Bona Fides	47
3.2.	Accuracy and Being Up To Date Where Necessary	47
3.3.	Being Processed for Specific, Explicit and Legitimate Purposes	48
3.4.	Being Relevant with, Limited to and Proportionate to the Purposes for Which They Are Processed.....	50
3.5.	Being Retained for the Period of Time Required.....	51
3.6.	Accountability	53

SECTION II

THE BASIS FOR THE CIVIL LIABILITY OF THE DATA CONTROLLER

1.	THE CONCEPT OF CIVIL LIABILITY	55
1.1.	Reasons of the Liability	57
1.1.1.	Fault	58
1.1.2.	Contract.....	58
1.1.3.	Provision of Law	58
1.2.	Liability for Protection of Personal Data	59
1.2.1.	Provisions of Liability in EU Legislations.....	59
1.2.2.	The Current State in Turkey.....	61

2.	THE LIABILITY OF THE DATA CONTROLLER ARISING OF THE TORT RELATION.....	65
2.1.	Unlawful Action of the Data Subject	66
2.1.1.	Unlawful Action.....	66
2.1.2.	The Lawful Grounds on the Processing of Personal Data	69
3.1.2.1.	Explicit Consent of the Data Subject	71
3.1.2.2.	The Conditions Provided by the Law Eliminating the Unlawfulness.....	76
3.1.2.3.	Compulsory States	77
3.1.2.4.	Necessity for the Conclusion or Fulfillment of a Contract	78
3.1.2.5.	Performance of the Legal Obligation	78
3.1.2.6.	Making Available to the Public.....	79
3.1.2.7.	Necessity for the Establishment, Exercise or Protection of a Right	80
3.1.2.8.	Legitimate Interest	80
3.1.2.9.	Assessment Concerning the Personal Data of Special Nature	82
2.2.	Damage as a Result of Processing of the Personal Data	83
2.3.	Causal Relationship between the Processing Activity and Damage	84
2.4.	Fault of the Data Controller	85
2.4.1.	Definition	85
2.4.2.	Fault in the Protection of Personal Data	86
2.4.2.1.	Fault of the Data Controller in EU Law.....	86
2.4.2.2.	Fault of the Data Controller in Turkish Law.....	89
3.	CONTRACTUAL LIABILITY OF THE DATA CONTROLLER.....	92
3.1.	Existence of a Valid Obligation Relationship.....	93
3.2.	Breach of Obligation by the Data Controller	97
3.2.1.	Obligations Arising of an Obligation Relationship.....	97
3.2.1.1.	Performance Obligations.....	97
3.2.1.2.	Secondary Obligations	99
3.2.2.	Data Controller's Activities that Breach the Contract	101
3.2.2.1.	Breach of Contract if Processing of Personal Data is a Performance Obligation	102

3.2.2.2.	Breach of Contract if the Performance of Processing or Protection of Personal Data is a Secondary Obligation	103
3.3.	Damage to Arise due to Breach of Contract	106
3.4.	Relation between the Breach of Obligation and Damage (Appropriate Causal Relationship)	108
3.5.	Data Controller's Fault.....	108
3.5.1.	Proof of the Fault	109
3.5.2.	Non-liability Agreement in the Processing of Personal Data	110
3.5.3.	Strict Liability of the Data Controller	111
4.	CULPA IN CONTRAHENDO LIABILITY OF THE DATA CONTROLLER	112
4.1.	Culpa in Contrahendo Liability in General	112
4.2.	Culpa in Contrahendo Liability in the Protection of Personal Data	115

SECTION III

ACTION FOR COMPENSATION AS A METHOD OF PROTECTION FOR THE PERSONAL DATA

1.	ACTION FOR COMPENSATION IN PROTECTION OF THE PERSONAL DATA.....	118
2.	TYPES OF ACTIONS FOR COMPENSATION.....	120
2.1.	Action for Material Compensation.....	120
2.1.1.	Determination of the Damage	122
2.1.1.1.	Material Damage	122
2.1.1.2.	Proof of Damage	123
2.1.1.3.	The Date to be Taken as the Basis in the Amount of the Damage	124
2.1.1.4.	Addition of Interest to the Damage	125
2.1.1.5.	Balancing.....	126
2.1.2.	Determination of the Compensation	128
2.1.2.1.	Factors Effecting the Material Compensation.....	128
2.1.2.2.	Reduction Reasons in the Material Compensation	130
2.1.3.	The Relation between the Action for Material Compensation and the Action for Agency Without Authority	133

2.2.	Action for Moral Compensation	134
2.2.1.	Theories Explaining Moral Damage Concept.....	136
2.2.2.	Moral Damage on the Basis of the Personal Data.....	139
2.2.3.	Determination of the Moral Compensation.....	140
3.	PARTIES OF THE ACTION FOR COMPENSATION	142
3.1.	Claimant	142
3.1.1.	Data Subject	142
3.1.2.	Relatives of the Deceased Person	144
3.2.	Defendant	146
3.2.1.	Natural Person Data Controller	146
3.2.2.	Legal Person Data Controller	146
3.2.2.1.	Evaluation for the Private Law Legal Persons	146
3.2.2.2.	Evaluation for the Public Law Legal Persons	147
4.	LIABILITY OF SEVERAL PERSONS FOR THE SAME DAMAGE (JOINT AND SEVERAL LIABILITY)	148
4.1.	The Liability of the Joint Data Controllers	149
4.2.	The Liability of the Data Processor	151
4.3.	Data Controller's Liability as an Employer	153
5.	STATUTE OF LIMITATION IN THE ACTION FOR COMPENSATION	157
5.1.	Statute of Limitation Arising of the Contractual Relation	157
5.2.	Statute of Limitation Arising of the Tort Relation.....	158
5.2.1.	Normal Term.....	158
5.2.2.	Maximum Term	159
5.2.3.	Exceptional Term.....	160
6.	AUTHORIZED AND COMPETENT COURT IN THE ACTIONS FOR COMPENSATION	162
7.	EFFECT OF THE PENAL COURT DECISION ON THE ACTION FOR COMPENSATION	162
8.	COMPETITION OF THE CONTRACT AND TORT RELATION	165
	CONCLUSION	168

ABBREVIATIONS

ACC	: Assembly of Civil Chamber
Art.	: article
Authority	: Personal Data Protection Authority
CC.	: Civil Chamber
Convention no 108	: European Council Convention no 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
COPPA	: The Children’s Online Privacy Protection Act
Directive no 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
D.	: Date
ECHR	: European Convention on Human Rights
Etc.	: et cetera
EU	: European Union
GDPR or Regulation	: Regulation of the European Union on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data
ICT	: Information and Communication Technology
LPPD	: Law on the Protection of Personal Data
OECD Guidelines	: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
OJ	: Official Journal
R.	: Resolution Number
Rec.	: Recital
RPPDECS	: Regulation on Protection of Personal Data in Electronic Communication Sector
TCC	: Turkish Civil Code

TCO	: Turkish Code of Obligations
TPC	: Turkish Penal Code No 5237
UN Guidelines	: United Nations Guidelines for the Regulation of Computerized Personal Data Files
Vol.	: Volume
Working Party	: Article 29 Data Protection Working Party



CIVIL LIABILITY OF DATA CONTROLLER FOR UNLAWFUL PROCESSING OF PERSONAL DATA

INTRODUCTION

1. The Significance and Objective of the Subject

In today's world, when a transition is made from the industrial age to information age¹, the one who has the information has a stronger position. The states need to collect the citizens' data for various reasons such as to assert more dominance over the citizens, to provide better public services, to collect the taxes, to plan the financial or health plans or to fight against crime². Private sector companies, on the other hand, tend to collect all data related to the consumers or people with consumer potential³. This way, they aim to achieve a better advertisement for their products, to offer products or services that target the habits or tastes of their consumers. In the information age, the private companies offering information services were established for the first time, and

¹ In this age, the standard instruments in the industrial economy were abandoned and instead, information producing and storing instruments such as computers, internet, were focused on. Information is in the center of economy and became the new raw material of the this age. The sources of power such as soil, labor, manufacturing instruments or factories in the industrial society were replaced by information. Yenal Ünal, "Bilgi Toplumunun Tarihi", *Tarih Okulu Dergisi*, Issue. 5 (2009), p. 124; A. Semih İşevi and Burçin Çelme, "Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak", *Bilgi Dünyası Dergisi*, Vol. V, Issue. 2 (2005), p. 256.

² The states need personal data in order to perform their legal activities arising of the constitution. The states processing the personal data of the citizens due to this need do not have unlimited freedom. A state should comply with the principles of the state of law while performing its duties, and should guarantee the fundamental rights and freedoms of the individuals. Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması* (Ankara: Beta, 2008), p. 5.

³ According to a research carried out in 2010 by *Eurobarometer*, which is responsible for the public researches of the European Union; 61% of the European citizens believe that they are required to disclose their personal data in order to access the websites offering online services such as social networks and social media websites. This rate goes up to 79% for internet shopping. The companies offering shopping over the internet generally process the names, home addresses and telephone numbers of their customers. 43% of the internet users believe that personal data more than required for accessing and using online services are requested. And again, according to this study, 70% of the Europeans have concerns that the data collected by the private companies may be used for the purposes other than the purpose for which such data were collected. Special EUROBAROMETER 359, *Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels, June 2011, p. 1-3. see: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf (Access Date: 15.07.2018).

information became a commercial product which could be purchased and sold⁴. The development of the information and communication technologies (*ICT*), increase of data storage capacities of the computers, simplification of data processing and analyzing and sharing such data with the third parties raised concerns with respect to the fundamental rights and freedoms of the individuals and accordingly, the issue of the protection of the personal data was brought to the agenda.

We can call the personal information such as our names, addresses, communication information, bank details, IP addressed, appearances, political opinions, and even shopping habits, likes, preferences, in short, all information concerning “us,” personal data⁵. Development of digital technology facilitates the storage, and usage of such data concerning us. Passing of the information, which is unique to us, into the hands of others and usage of such information for their benefits without our knowledge and consent is considered as a severe blow in terms of privacy of the modern man. The realm of freedom of an individual, who is uninterruptedly tracked, observed, whose behavior profile is determined and oriented, shall be narrowed down if specific legal and technical measures are not taken.

Due to these reasons, a legal provision was required in order to determine the method of the protection of the personal data, the extent of such protection, and the limitations of the processing. The purpose of the protection of personal data is to provide that the companies and the states accomplish the free movement of the information within a safer legal system in compliance with the reality of the advancing technologic process and the era as well as protection of the fundamental rights and freedoms of the individuals⁶. For these purposes, the method and conditions of processing the

⁴ Ünal, p. 132.

⁵ Elif Küzeci, *Kişisel Verilerin Korunması*, 2.Edition (İstanbul: Turhan Kitabevi, February 2018), p. 1.

⁶ Henry Pearce, “Big Data and the Reform of the European Data Protection Framework: An Overview of Potential Concerns Associated with Proposals for Risk Management-based Approaches to the Concept of Personal Data”, *Information & Communications Technology Law*, Vol. 16, Issue. 3 (2017), p. 314; Douwe Korff, “Practical Implication of the new EU General Data Protection Regulation for EU and non-EU Companies”, *Final Report*, Cambridge: Commission of the European Communities, (1998), p. 3-7. see: <https://ssrn.com/abstract=3165515> (Access Date: 25.08.2018); Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması* (Ankara: Çakmak, 2010), p. 75. Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması* (Ankara: Yetkin, 2004), p. 31; this is also expressed in the General Preamble section of the Law on the Protection of Personal Data no 6698. Lack of general data protection legislation in our country for a long time also prevented the

information, the obligations of the data controller, and the rights of the data subject are regulated by the law on the data protection⁷. The individuals shall share their data without any concerns in the societies where the personal data of the individuals are stored safely, and the public and private sector shall realize the free movement of the information within the frame of the data protection limits.

The objective of the law on the protection of personal data is to take preventive measures before the individual's personal rights are violated⁸. Accordingly, legal provisions for lawful processing of the personal data were designed in order to prevent any attack on personal rights. Although the processing of personal data is defined as an unlawful act in principle, the principles and conditions for processing such personal data were determined by these legal provisions and unlawfulness was eliminated accordingly. Moreover, definitions concerning the personal data were made, and some uncertainties in the field of law on data protection, which is a new emerging area, were clarified. Consequently, the third parties were tried to be prevented from acquiring our personal data, and the dominance of the individuals on their data was strengthened.

As mentioned above, the law on the protection of personal data is the rules of law regulated in order to prevent an attack on the personal rights of the individuals. However, many provisions were made in our law in order to protect those whose personal rights are violated due to the processing of personal data despite these provisions. In this day and age in which the fundamental rights and freedoms of the individuals including the right to privacy, can easily be violated through the processing of personal data, it is required to draw the boundaries of the types of sanctions to be applied as a result of such violations. Although the sanctions of these violations are clearly regulated within the frame of both the criminal law and administrative law, private law does not set forth the sanctions, and it refers to the general principles. In our study, the answers to the questions of how the losses to arise of the violations concerning the protection of personal data would be compensated by the Turkish Civil Code (*TCC*), and Turkish Code of Obligations (*TCO*) are tried to be found.

effective management of the investments of the foreign capital in other countries as well as our country, which was a deterrent factor for the foreign capital to invest in our country.

⁷ Aidan Forde, "The Conceptual Relationship Between Privacy and Data Protection", *Cambridge Law Review* (2016), p. 138.

⁸ Başalp, *Kişisel Verilerin Korunması*, p. 31.

2. Boundaries of the Research

The issue of the protection of personal data is an interdisciplinary issue. It closely concerns law as well as concerning the branches of science such as informatics engineering, politics, and sociology. The legal aspects of the issue shall be examined in our present study. However, this issue extends over to all the branches of law as well. Since the Turkish Constitution protects personal data within the frame of the fundamental rights and freedoms, this issue is also essential for the Constitutional Law. The results of the unlawful acquisition and processing of the personal data are, in principle associated with the violation of personal rights within the frame of the Civil Code. The provisions in the articles 23-24 and 25 of TCC protecting the personality are significant concerning the private law sanctions to occur as a result of data breaches. This is expressed as “*The right to compensation under general provisions of those whose personal rights are violated is reserved*” in the art. 14/3 of the Law on the Protection of Personal Data No 6698 (LPPD or Law no 6698)⁹.

On the other hand, protection of the personal data can be imposed as an obligation on one party within a contractual relationship between the parties. In this case, unlawful processing or non-protection of the personal data shall constitute contrariety to the obligation. Due to this reason, it is required to consider the issue within the scope of the civil code and the code of obligations.

Besides, the administrative sanctions are regulated separately for each violation within the scope of the LPPD art. 18¹⁰. The Penal Code sanctions were first regulated in 2005 under the articles 135 to 140 of Turkish Penal Code No 5237 (TPC)¹¹. Within the scope of these articles, unlawful collection, recording and disclosure of personal data are regulated as a crime.

⁹ No: 6698, Adoption D.: 24.03.2016, O.J: 29677, T: 07.04.2016. Shall be referred to as LPPD hereinafter.

¹⁰ The limits of the administrative sanctions are stated one by one in the article 18 of LPPD. According to this article; an administrative fine from 5,000 Turkish Liras up to 1,000,000 Turkish Liras can be imposed by the Personal Data Protection Authority (Authority) on the data controllers processing the personal data unlawfully. It is stated that these fines shall be applied for the natural persons and private law legal persons who are the data controllers.

¹¹ Consideration of unlawful processing of personal data as a crime was brought with the Turkish Penal Code no 5237 which took effect on June 01, 2005. No such regulation existed in the cancelled TPC no 765.

Liability for compensation within the frame of the civil law of the data controllers, who unlawfully collect, process the personal data and transfer these to the third parties, shall constitute the focal point of our study. Even if awareness was created thanks to various conferences concerning the issue of the protection of personal data organized in our country in the recent periods and the obligation to inform policies applied by some companies for the customers, the individuals usually do not exercise their rights to compensation with respect to the violations they encounter¹². How the damages of the data subjects shall be compensated in case of data violations by the private law legal persons shall be examined in the conclusion of this study.

3. The Plan of the Research

The personal data concept shall be defined in the first section with the title “*The Concepts and Fundamental Principles Concerning the Personal Data*” and the fundamental concepts concerning our study shall be examined, especially the identity of the data controller shall be explained and the differences between the data processor and data controller shall be mentioned. The categories of personal data shall also be explained since these would change the conditions of unlawfulness and the personal data of special nature and ordinary personal data shall also be described within this frame. Moreover, the legal nature of the personal data shall be mentioned, and opinions about the legal nature of the personal data in America, Europe, and Turkey shall also be included. Finally, the fundamental principles for the processing of the personal data shall be described under the light of the international and national legislation.

In the second section of our study, the civil liability of the data controller shall be examined under the title “The Basis for the Civil Liability of the Data Controller.” In this section, “Civil Liability” concept, in general, shall be examined first, and then the conditions of civil liability arising from the processing of the personal data accurately shall be described. In this section, the tort liability of the data controller and the

¹² According to survey of *Eurobarometer* carried out in 2010; only 33% of the European citizens were aware of the existence of a national public authority responsible for the protection of their rights concerning the personal data. When it is considered that the awareness is so low although the rules for the protection of the personal data existed in Europe much earlier than our country, the low level of awareness, it can be concluded that the awareness of our citizens concerning the protection of personal data is lower considering that the Law on Protection of Personal Data took effect in our country only in 2016. Special EUROBAROMATER 359, p.1-3.

conditions of the tort liability shall be examined within the frame of the protection of the personal data. Moreover, in this section, the results of the data controller's actions that are contrary to the obligation, when there is a legal relationship between the data controller and the data subject, shall be examined. Finally, the data controller's *culpa in contrahendo* liability shall be described.

In the final section, the compensation of the damages incurred by the data subject as a result of the data controller's processing activities such as collection, recording, storage of the personal data unlawfully or transferring these to the third parties, shall be concretely discussed. First of all, the types of actions for compensation filed as a result of the civil liability mentioned in the second section shall be examined. During such explanations, detailed examples shall be given in order to enable a better understanding for the readers. In the final section of our research, the procedural parts such as the parties of the action for compensation, the cases in which more than one person is responsible for the same damage, statute of limitation and competition of demands shall be described briefly, and our research shall be concluded.

4. Sources of the Research

The issue of the protection of personal data was addressed both in the doctrine and in the reports of the international or national institutions or in the court decisions starting from the end of the 1960s. Many legal provision were created concerning this issue. While preparing this study, mainly the sources of law were used, but the studies in the fields of sociology, informatics, and economy were also benefitted from. However, since our study is about the evaluation of the protection of personal data for civil law, the sources of law constitute the backbone of our study.

Within this frame, international and national legislation was examined first in order to determine the essential qualities of the personal data. The primary international legislations constituting the personal data protection law were carefully studied, and the works related to these were benefitted from. Accordingly, the leading international sources referred to in order to conclude our research are;

“European Convention on Human Rights¹³(ECHR)”, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ¹⁴(OECD Guidelines)”, “European Council Convention no 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data¹⁵(Convention no 108)”, “United Nations Guidelines for the Regulation of Computerized Personal Data Files ¹⁶(UN Guidelines), “Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data¹⁷ (Directive no 95/46/EC)” and finally “Regulation of the European Union on the Protection of Natural Persons with regard to the processing of Personal Data and on the Free Movement of Such Data ¹⁸ (GDPR or Regulation)”. In the national regulations, while Law on Protection of Personal Data no 6698, which was just put into effect, is significant, Turkish Civil Code and Turkish Code of Obligations were

¹³ European Convention on Human Rights, for the full text see: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Access Date: 19.08.2018).

¹⁴ The mentioned regulation is important for being the first international document concerning the protection of personal data. Mainly economic benefits are observed. OECD, “Guidelines on the protection of privacy and transborder flows of personal data”, <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> (Access Date:19.08.2018).

¹⁵ This is the first binding international convention. Turkey is also a party to this convention. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981. see;

<https://www.coe.int/en/web/conventions/full-list/?conventions/rms/0900001680078b37> (Access Date: 19.08.2018) For detailed information about this convention see: Esra Tekil Yıldız, “İnternet Üzerinde Kişisel Verilerin Korunması”, *Prof. Dr. Fahiman Tekil’in Anısına Armağan* (İstanbul, 2003), pp.791-793.

¹⁶ United Nations, “Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990. see: <http://www.refworld.org/pdfid/3ddcafaac.pdf> (Access Date:19.08.2018)

¹⁷ This directive is benefitted from in preparation of the Law on Protection of Personal Data no 6698. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. see;

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> (Access Date: 19.08.2018) .

¹⁸ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). see:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (Access Date:19.08.2018) The Regulation was directly applied in EU member states as of May 25, 2018. For the general information about the Regulation see: The United Kingdom Information Commissioner’s Office (ICO), *Overview of General Data Protection Regulation*, London, 2016, see: <https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf> (Access Date: 25.08. 2018).

the essential legislation in solving the problem of compensation arising of the violation of personal data

Many publications and researches concerning the subject of our research were benefitted from, and our studies were shaped within the direction of the decision of both the Supreme Court and the Court of Justice of the European Union (CJEU). Up to date, discussions concerning the subject of the research were found over the internet sources, and these discussions were evaluated. Accordingly, the subjects we handled were tried to concretize in the readers' minds.

Moreover, the references were made to the reports of the European Union Article 29 Data Protection Working Party, (*Working Party*) European Union Data Protection Supervisor ¹⁹ and other institutions of the EU, and finally, the working reports of the Personal Data Protection Authority established in 2016 were taken into consideration in the present research.

¹⁹ European Union Data Protection Supervisor is the independent data protection authority of the European Union established under the GDPR, which performs activities in place of the Working Party established as based on 29th Article of the directive no 95/46.

SECTION I

THE CONCEPTS AND FUNDAMENTAL PRINCIPLES CONCERNING THE PERSONAL DATA

1. THE CONCEPT OF PERSONAL DATA AND ITS LEGAL NATURE

1.1.The Concept of Personal Data

The concept of personal data is defined by national and international legal regulations. In compliance with art. 4/1 of the GDPR, the concept of personal data is defined as “*any information relating to an identified or identifiable natural person.*” There is a general provision in the international regulations concerning the definition of personal data²⁰. These definitions were influential in many countries for the regulation of their domestic laws and were transferred in the same manner. However, the extensive nature of the definition resulted in different interpretations concerning the factors of personal data²¹.

In compliance with the art. 3/1 of the Law on the Protection of Personal Data no 6698, which is quoted by a very few changes from the Data Protection Directive 95/46/EC, personal data is “*all the information relating to an identified or identifiable natural person.*” On the other hand, it is defined as “*all the information relating to identified or identifiable natural or legal persons*” in the Regulation on Protection of Personal Data in Electronic Communication Sector²² (RPPDECS) which took effect on June

²⁰ The personal data are defined in the same manner in Convention no108, OECD Guidelines and the Directive 95/46/EC. see: Convention no 108, art. 2/a; OECD Guidelines, art. 1/b; Data Protection Directive 95/46/EC, art. 2/a.

²¹ Pearce, p. 315; Çiğdem Ayözger, *Kişisel Verilerin Korunması-Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil* (İstanbul: Beta Yayınları, 2019), p. 5.

²² O.J: 28363, D: 24.07.2012, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0> (Access Date: 22.02.2018).

24, 2012. Again in the LPPD's preamble,²³ “*all the information appropriate for making the identity of individuals identifiable*” is defined as personal data. It can be stated within the frame of the provisions in the legislation that all information relating to and identifying or having the potential to identify a person is called personal data.

Within the direction of these definitions, two essential features to distinguish the personal data and non-personal data is that such data are related to one person and that such person is identified or identifiable²⁴. Such information covers all the points that can be associated with the concerned person such as the names, surnames, ethnical origin, political opinion, sexual preferences, shopping habits, addresses, insurance numbers, registrations and even the teams they support.

As can be understood from these explanations, personal data is not considered as limited in the normative legal order²⁵. However, samples to the personal data were given in one part of these provisions. After defining the personal data in art. 4 of GDPR, it was stated that “*an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*” can be personal data. Moreover, it is explained in the LPPD's preamble that the information related to the individual's physical features, family, economic, social and other characteristics can be assumed as personal data in addition to the information such as the name, surname, date of birth and place of birth, which enables the definite identification of the individual.

The most important reasons that the personal data are not assumed as limited in the laws are the impossibility to predict what the data that can be associated with the

²³ Draft Law on the Protection of Personal Data (1/541) and Committee on Justice Report (LPPD's Preamble), Order No: 117 <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> (Access Date:22.02.2018).

²⁴ Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku* (İstanbul: Hukuk Akademisi, 2019), p. 4; Küzeci, s. 9.

²⁵ Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması* (İstanbul: Onikilevha Yayıncılık, 2017), p. 27.

individual shall be and the desire to present a new data definition which will also cover the data categories to emerge together with the advancing technology²⁶.

Although the definition of the personal data is almost similar in the international and national regulations, the determination whether the data are within the scope of the personal data is made by a proper subjective evaluation due to the broadness of this definition²⁷. Due to this reason, the factors of the personal data were listed differently through interpretation in implementation and doctrine. One of the most important reasons for this is that such factors are nested in practice and are feeding each other²⁸.

Working Party examined the factors of the personal data under four main titles as *any information, relating to, an identified or identifiable and natural person*²⁹. We shall examine the personal data under three main titles as information, and identified or identifiable person and relating to a person³⁰.

1.1.1. Information

The concepts of data and information which are among the most important concepts of the information society³¹ constitute the keystones of the personal data protection law. The concepts of information, and data are frequently used in the personal data protection law and several mistakes are made in the use of these concepts³². Due to this reason, it will be beneficial to examine these concepts.

²⁶ Dülger, p. 12; Personal Data Protection Authority, *6698 Sayılı Kanunda Yer Alan Temel Kavramlar*, Ankara, 2017, p. 10. For this guide, see: <https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20KANUN%E2%80%99DA%20YER%20ALAN%20TEMEL%20KAVRAMLAR.pdf> (Access Date: 10.07.2018).

²⁷ Due to this reason, although the member countries transferred the same definition to their domestic laws during the time of the Directive no 95/46/EC, the implementation and doctrine was resulting in different interpretations in determination of the factors of the mentioned definition. Aksoy, p. 12. Today, as GDPR took effect, it was aimed to develop a single case law in protection of the personal data and the emergence of different interpretations between the member countries was tried to be prevented.

²⁸ Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, Brussels, 2007, p. 6. For this report see: <https://www.pdp.ie/docs/1030.pdf> (Access Date:03.05.2018).

²⁹ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 6.

³⁰ In the doctrine, the factors of the personal data are generally described under these three titles. see: Dülger, p. 5-12.

³¹ This concept is also expressed in the doctrine by the concepts such as; the third wave, post-modernity society, post-bourgeois society, post-economy society, post-industrial society, information society, personal service society. see: Ünal, p. 132.

³² Russel Ackoff, "From Data to Wisdom", *Ackoff's Best*, John Wiley & Sons, 1999, p. 170-172; İşevi and Çelme, p. 263.

Data is defined as “*display of the facts, concepts or commands in an appropriate manner for communication, interpretation, and processing.*”³³ This form of the display can be as numbers, ciphers, writings, graphics or pictures. Data is everything that reaches us from what exists. Everything, like the sound of the rain, the number of people, the books we have, the color of the clothes we wear and the feelings of people is data. Information is “*the meaning attributed by the individual to the data by the use of certain rules.*”³⁴ Again according to another definition; “*information is the data processed in a meaningful manner for the receiver.*”³⁵ Within this context, we can say that data is the unprocessed, raw form of information³⁶. Information is a more useful form of data. For instance, while the indications acquired by the census-takers about the individuals are data, and information is obtained by interpretation of such data at the census bureau and conversion of them into statistical charts³⁷.

For any information to be considered as personal data associable with a person, it is not required to be private information³⁸. The information concerning individual’s opinions, physical features, clothing which is publicly presented can be processed as personal data whereas the most private information such as health problems, sexual life or nude photographs can also be processed as personal data³⁹. Due to this reason,

³³Türk Dil Kurumu, *Güncel Türkçe Sözlük*, <http://sozluk.gov.tr/?search-input=veri> (Access Date:11.04.2018); Another definition for the concept of data is as, “*raw information not meaningful or used singly, but which requires association, grouping, construction, interpretation and analysis constituting the basis for the information*”. Malik Yılmaz, “Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi”, *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, Vol. XLIX, Issue. 1 (2009), p. 98.

³⁴Türk Dil Kurumu, *Güncel Türkçe Sözlük*, <http://sozluk.gov.tr/?search-input=veri> (Access Date:11.04.2018)

³⁵ Küzeci, p. 11.

³⁶ İşevi and Çelme, p. 263. As could be understood from these definitions, although the concepts of data and information have different meanings, both concepts are used interchangeably in the Directive or Regulation or national legal regulations. Aksoy, p. 11; Ackoff, p. 170.

³⁷ Ackoff, p. 170.

³⁸ Erbil Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması* (İstanbul: Onikilevha Yayıncılık, 2017), p. 51; Aksoy, p. 14; Taştan, p. 37; İlke Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı* (Adalet Yayınevi: İstanbul, 2016), p. 8.

³⁹ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 7; Yıldız, p. 787; The right for the protection of personal data is beyond the right of respect for the private and family life. Although the European Court of Human Rights mentioned in one decision that the concept of private life should be interpreted broadly, the protection of personal data regulated in the art. 8 of the European Union Fundamental Rights is taken as a different right independent of the right to Respect for Private Life regulated by the art. 7. For the mentioned decision of the European Court of Human Rights, see: ECHR, *Amann v Switzerland*, 16.02.2000, 27798/95, <https://www.legal-tools.org/doc/6e49ed/pdf/> (Access Date: 15.07.2018).

the right for the protection of personal data and the right for the protection of privacy do not entirely match up.

If the parameters of being identified or identifiable person or being related to a person, which are required for any information to be considered as personal data, exist, then these can be assumed as personal data without considering whether such information is correct or not⁴⁰. For instance, the information that a person has epilepsy can be accepted as personal data even if it is not correct. Thus the fiancé/fiancée learning this information may leave such person, or this can prevent such person from being employed⁴¹.

The subjective or objective character of information does not have any influence on the qualification of such information as personal data⁴². The information containing subjective opinion or evaluations about a person constitutes a significant part of personal data processing in many sectors. For example, the expressions concerning a person such as being reliable (*banking sector*), expected to die (*insurance sector*) or be a good employee (*employment sector*) are accepted to be personal data⁴³. In addition to these, processing of objective information such as penal conviction decisions, being AIDS patient is also within the scope of personal data.

1.1.2. Identified or Identifiable Person

The second factor of personal data is the person factor. The person is the being who benefits from the rights and is the owner of such rights⁴⁴. In private law, the opinion that there can be no person possessing no rights as well as that there can be no rights not belonging to any person is dominant⁴⁵.

⁴⁰ Beytar, p. 51, Article 29 Data Protection Working Party, *The Concept of Personal Data*, p.6.

⁴¹ As it shall be mentioned hereinafter, the requirements of the accuracy and, if required, up to dateness of the personal data were brought by the art. 4 of the LPPD and the easy access of the data subject to the data and the right to demand correction of these if such are incomplete or processed falsely were brought by the art. 12 of the LPPD in order to prevent such conditions.

⁴² Aksoy, p. 14; Taştan, p. 38.

⁴³ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 6.

⁴⁴ Rona Serozan, *Medeni Hukuk, Genel Bölüm/ Kişiler Hukuku* (İstanbul: Vedat Kitapçılık, 2017), p. 415; Serap Helvacı, *Gerçek Kişiler*, 8. Edition (İstanbul: Legal Yayınları, 2017), p. 21.

⁴⁵ M. Kemal Oğuzman, Özer Seliçi and Saibe Oktay-Özdemir, *Kişiler Hukuku- Gerçek ve Tüzel Kişiler*, 17.Edition (İstanbul: Filiz Kitabevi, 2018), p. 1.

The most critical issue discussed within the scope of this concept, whether the term, data subject, includes the legal persons as well as natural persons⁴⁶. The definitions in GDPR and LPPD are regulated as “*all information related to the identified or identifiable natural person.*” Accordingly, the concept of person is limited by natural person.

On the other hand, both the legal and natural persons were accepted to be the data subjects in the definition of the personal data in the European Council Directive no 2002/58/EC⁴⁷ and the RPPDECS. Consequently, both the legal persons and natural persons are protected in the areas concerning the electronic communications sector.

There are various discussions on whether to include the legal persons within the scope of the data subject⁴⁸. According to one opinion, the protection of the legal persons within the scope of LPPD shall constitute contrariety to the purpose of the law⁴⁹. The issue of the protection of personal data emerged out of the protection of fundamental rights and freedoms, including the right to privacy. As a result, the protection of the legal persons contradicts the underlying logic of these regulations. Since this shall reduce the concern for the protection of human rights, it shall damage the protection of the natural persons within the frame of human rights⁵⁰.

According to another opinion believing that the legal persons should not be considered within the frame of the general personal data protection, although the legal persons are also included within the scope of the protection in the Directive no 2002/58 or in RPPDECS, such regulations could be implemented only in specialized areas. The protection of the legal persons is appropriate in some special regulations in order to

⁴⁶ For detailed information about this subject see: Korff, pp. 56- 59.

⁴⁷ Directive 2002/58/EC of the European Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector dated 01,12,2002, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> (Access Date: 13.04.2018) TR’de tarihi kelimesi küçük harf ile yazılmış.

⁴⁸ For exclusion of legal persons from the scope of the protection of personal data see: Dülger, p. 9; Küzeci, p. 326; Şimşek, p. 207; Ayözger, p. 10; Durmuş Tezcan, “Bilgisayar Karşısında Özel Hayatın Korunması”, *Anayasa Yargısı*, Vol. 8 (1991), p. 389. For the counter-opinion see: Başalp, *Kişisel Verilerin Korunması*, p. 109; Ian Walden and Nigel Sawage, “Data Protection and Privacy Laws: Should Organisations be Protected?”, *International and Comparative Law Quarterly*, Vol. 37, Issue. 2 (April 1988), pp. 337-347; Taştan, p. 30.

⁴⁹ Küzeci, p. 325; Ayözger, p. 10.

⁵⁰ Tezcan, p. 389; Küzeci, p. 326; Dülger, p. 9.

protect the legal interest of the legal persons as based on the qualities of these areas⁵¹. This way, these regulations shall be complementary for the general data protection laws.

According to the opinion believing that the personal data protection law should also include the legal persons since immaterial damages can be demanded if the reputation of the legal person is damaged, it is also required that the personal data of the legal persons should also be protected against unlawful processing⁵². The protection of personal data of the legal persons is generally considered in our laws within the scope of “trade secret⁵³.” For the information of the legal persons to be protected within the frame of the trade secrets, such information is required to be non-public which the owner desires to remain confidential⁵⁴. However, the scope of the information to be processed concerning a natural person is more extensive than the protection of the personal data of the legal persons. Accordingly, not only the person’s information within the secret area but also the information within the scope of private area⁵⁵ and even non confidential, public data are also included within the scope of the protection. The majority of the international regulations concerning the data protection include only the natural persons as the data subject within the scope of the protection⁵⁶. International regulations generally determine the minimum standards concerning the protection of the personal data, and providing protection above these standards was left up to the discretion of the Member States. Due to this reason, the legal persons are also protected in the personal data protection legislation of some States⁵⁷. Although

⁵¹ Ayözger, p. 10.

⁵² Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu* (İstanbul: Onikilevha Yayıncılık, 2018), p. 21.

⁵³ Trade secret is defined as; “*information with an independent value, providing competitive advantage for the owner, known only within a limited environment, and of which its confidentiality is beneficial for the owner*”. Mehmet Emin Bilge, *Ticari Sırların Korunması* (Ankara: Asil Yayıncılık, 2005), p. 5; Muhammed Sulu, *Ticari Sırların korunması* (İstanbul: Onikilevha Yayınları, 2016), p. 12.

⁵⁴ Bilge, p. 5.

⁵⁵ The scope of the private life is wider than the secret area of a person. For detailed information about this see: Aksoy, p. 47-54.

⁵⁶ See: Convention no 108, art. 2/a; OECD Guidelines, art. 1; EU Directive o 1995/46 EC art. 3.

⁵⁷ For example, in a study dated 1998, the legal persons are also protected by the legislations related to the protection of personal data in EU member countries such as Austria, Denmark, Italy and Luxembourg or in non-EU member countries such as Iceland, Norway and Switzerland. For detailed information see: Korff, p. 1-2. Determination of the scope of the concept of person is important for determining who shall benefit from the legal protection in the data protection laws. According to LPPD,

legal persons are not protected under LPPD, if any natural person can be reached by the data of the legal persons, then such data are also considered as personal data⁵⁸.

1.1.2.1. Protection of the Children's Personal Data

Today, in which the information and communication sector progressed enormously, the personal data of the individuals can be processed easier. Those who are affected most by this situation are the children⁵⁹. As internet users, children occupy a significant place, and this makes them an open target for the processing of their personal data⁶⁰. According to the researchers carried out, it is believed that the children leave more personal data on the online mediums when compared to the adults, and are less aware of the personal data processing risk⁶¹. This condition whets the appetite of those people who desire to use such personal data for their benefits⁶². Due to this reason, they become exposed to the loss of reputation, commercial exploitation of personal data, identity theft, cyber-attacks, determination of the profiles⁶³.

the legal persons shall not have the rights of the data subject which are regulated by the law. Aksoy, p. 18.

⁵⁸Dülger, p. 10; Başalp, *Kişisel Verilerin Korunması*, p. 35. For the critics on distinguishing the legal person-real person in protection of personal data see: Walden ve Sawage, pp. 337-347.

⁵⁹ In compliance with the art. 1 of the UN Convention on the Rights of the Child, *a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier*. For the mentioned Convention, see: https://www.ohchr.org/en/professional_interest/pages/crc.aspx

⁶⁰ According to one research, each one of three internet users is anticipated to be below the age of 18. Sonia Livingstone, John Carr and Jasmina Byrne, "One in Three: Internet Governance and Children's Rights", *Global Commission on Internet Governance Paper Series*, No. 22 (2015), see: https://www.cigionline.org/sites/default/files/no22_2.pdf (Access Date: 20.02.2019)

⁶¹ Milda Macenaite and Eleni Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?", *Information & Communications Technology Law*, Vol. XXVI, Issue. 2 (2017), p. 147; This condition is also expressed in the recital 38 of GDPR.

⁶² According to a research, personal data of the 9% of the children between the ages 11-16 living in Europe are processed unlawfully and exploited. Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson, "Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 Year Olds and Their Parents in 25 Countries", *EU Kids Online, Deliverable D4. EU Kids Online Network* (London 2011). In order to access the report, see: <http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28Isero%29.pdf> (Access Date: 03.11.2018).

⁶³ Milda Macenaite, "From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation", *New Media and Society*, Vol. 19, Issue. 5 (2017), p. 765.

There are provisions in GDPR which are specifically for the personal data of children⁶⁴. According to art. 8/1 of GDPR, in cases where consent is applicable due to the lawfulness reasons, the processing of the personal data of a child shall possible with the consent of the child where the child is at least 16 years old, and such consent alone shall not be sufficient where the child is below the age of 16 years. However, such processing shall be applied if and to the extent the consent is given by or authorized by the holder of parental responsibility for the child. GDPR gave the Member States the right to lower this minimum age limit, on condition not to be smaller than 13 years old⁶⁵.

There is no special provision in LPPD concerning the protection of the personal data of the children. Due to this reason, children are under the same level of protection with the other data subjects⁶⁶. However, stricter and more special provisions are made with respect to the protection of the personal data of children, when the developments in Europe and the world are examined⁶⁷. This way, the future risk of the aftermath of the decisions given at a minimum age by the children sharing their data unconsciously was tried to be prevented. Accordingly, it is also required in our country to have special provisions for the protection of the children's personal data.

If the concept of consent for the processing of the children's personal data in Turkey is to be mentioned, consent for the processing of personal data can be considered as a right that is tightly connected to the individual. The minimum age limit for which the consent of the child applies for the processing of the personal data is not regulated in LPPD. Due to this reason, general provisions shall be referred to. If the child is capable of understanding the results of the personal data processing activity, in other words, if

⁶⁴ "The Children's Online Privacy Protection Act (COPPA) in 1998" law concerning the protection of children's privacy on online platforms is in effect in America. Special protection provisions for the children are prepared in GDPR by taking this law into consideration. For this law, see:

<https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5> (Access Date: 12.01.2019).

⁶⁵ For detailed information, see: Macenaite and Kosta, pp. 146-197; According to European Data Protection Supervisor the consent of the legal representatives is a reasonable approach for processing of the personal data of the children below the age of 13. European Data Protection Supervisor, *The Data Protection Reform Package*, Brussels, 2012, p. 21.

⁶⁶ Protection provisions special for children were not regulated also in the Directive no 95/46/EC.

⁶⁷ In the Recital 38 of GDPR, it was clearly emphasized that children should be protected more. The Regulation provided for making the appropriate notifications for the children, establishment of stricter rules with respect to oblivion right and stronger protection for the marketing and profiling activities. Macenaite and Kosta, p. 148.

the child is assumed to have the discriminative capability for such activity, then the child's consent for the processing of personal data shall be considered as lawful. Due to this reason, whether the consent of the child in the processing of children's personal data is a reason of lawfulness or not shall be variable based on the case in question. If it is accepted that the child is not capable of discrimination for the case in question, then the personal data cannot be processed unless with the consent of the child's parents or legal guardians.

1.1.2.2. Opinions on Protection of the Personal Data of Deceased Persons

Another important issue discussed within the scope of the personal data protection law is about how the personal data of the deceased persons would be protected. LPPD No 6698 makes provisions for the natural persons. However, there is no provision concerning the protection of the personal data of the deceased person. In Recital of 27 of GDPR, it is stated that the protection of the personal data of the deceased persons is not within the scope of this Regulation. However, the Member States were given the right to expand the scope of the Regulation and include the personal data of the deceased persons within the scope of the Regulation.

Since there is no such provision in LPPD for the deceased persons, the personal data of such people should be protected according to the general provisions within the scope of the personal values of the deceased persons. This should be examined within the frame of the discussions in the civil law concerning the post-mortal protection of the values of personal rights⁶⁸.

According to these arguments, the personal values of the deceased person end. However, there are discussions in the doctrine whether the ending of the personal values would or would not mean that such a person also loses the right for protection of personal values. According to widespread opinion in Turkish/Swiss law, the protection of the personal values of a person ends by death. However, if any attack on

⁶⁸ Nafiye Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", *İÜHFİM*, Vol. LXXV, Issue. 2 (2017), pp. 765-790; For detailed information about these discussions see: Halil Akkanat, *Ölümün Özel Hukuk İlişkilerine Etkisi* (İstanbul: Filiz Kitabevi, 2004); Ümit Gezder, "Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliği Koruma Teorisi", *İÜHFİM*, Vol. LXV, Issue.1 (2007); Hasan Petek, *Kişilik Değerlerinin Ölümden Sonra Korunması* (Ankara: Yetkin Yayınları, 2015).

the personal values of a deceased person results in a violation of the personal rights of the deceased person's relatives (protection of the memory), then it is possible for these relatives to file cases in their own names⁶⁹. This indirectly expresses the protection of the personal values of the deceased person⁷⁰.

According to the decisions of the German courts specifically⁷¹ and another opinion defended by the doctrine⁷², post-mortal protection of personal rights should be direct. According to this opinion, the belief that the personal rights of a person shall not be destroyed following the death of such person should also be considered as a personal right⁷³. This way, while the person is still alive, he/she shall be sure that his/her personal rights shall not be violated after his/her death and shall be able to develop his/her personality freely⁷⁴. For example, a person having a social media account may not share anything fearing that third parties may log into his/her account after his/her death. Thanks to the protection of personal rights after death, logging into the social media account of the deceased person shall continue to constitute a violation of personal rights. Since the unlawful violation of the personal data constitutes an attack to the personal rights, the inheritors or the relatives of the person may protect the rights of the deceased person⁷⁵.

1.1.2.3. Protection of the Unborn Children within the scope of the Personal Data Protection Law

The development of genomic science and pre-birth treatment techniques in today caused arguments on whether the personal data of the fetus in the mother's womb should be protected or not during the processing of the genetic data of the fetus. During many clinical activities carried out with the mothers, many medical data related to the

⁶⁹Helvacı, *Gerçek Kişiler*, p. 101; Oğuzman, Seliçi and Oktay-Özdemir, p. 251; Taştan, p. 32.

⁷⁰ Gezder, *Ölüm Sonrası Hatırayı Koruma Doktrini*, p. 211.

⁷¹ The personal rights of a deceased person were first protected by Mephisto Decision of the German Federal Court. BGH, Urteil vom 20. März 1968- I ZR 44/66- BGHZ 50, p. 133 ff; Gezder, *Ölüm Sonrası Hatırayı Koruma Doktrini*, p. 207; Petek, p. 91.

⁷² For the authors favoring this opinion in Turkish Law see: Akkanat, p. 86-87; Bilge Öztan, *Şahsın Hukuku Hakiki Şahıslar*, 9.Edition (Ankara: Turhan Kitabevi, 2000), p. 25.

⁷³ Gezder, *Ölüm Sonrası Hatırayı Koruma Doktrini*, p. 215.

⁷⁴ Petek, p. 90.

⁷⁵Önder Kutlu and Selçuk Kahraman, "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, Vol.5, Issue.4 (2017), p. 55; Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması* (Ankara: Seçkin Yayınları, 2009), p. 291.

reactions given to the treatment by the fetus in the mother's womb may be processed. In this case, what should be the scope of the protection of the data related to the fetus? There are no provisions both in LPPD and GDPR concerning this issue⁷⁶.

There is no clear provision in GDPR and LPPD concerning the fetus. Although it is regulated by the Rec. 27 of GDPR that the deceased persons shall not be protected within the scope of this Regulation, there are no provisions concerning the fetus. The lawmakers could have clearly regulated that the unborn children shall not be protected within the scope of this Regulation just like they regulated that the data concerning the deceased persons shall not be protected within the scope of this Regulation. However, no such provision was made, so it could be considered that the personal data of the unborn children are protected within the scope of the Regulation⁷⁷. On the other hand, the definition of the natural person given in the Regulation does not clearly express it as a living person. Due to this reason, it can be concluded that the Regulation left the door open concerning this issue and desired to shape the protection of the personal data of the fetus as based on the problems in the practice and the court decisions.

With respect to Turkish Law, there is no special provision concerning the unborn children in LPPD. Accordingly, the mentioned issue should be solved in compliance with the provisions of the general law, TCC, protecting the personality. According to art. 28/II of TCC, "*The child possesses the right of capacity at the very moment he/she enters mother's womb (as a fetus) provided that he/she is born alive.*". According to this provision, the fetus's right of capacity is linked to the dilatory condition which is to born alive⁷⁸. In other words, as the dilatory condition of live-born takes place, the

⁷⁶ The first international regulation for the protection of the personal data of fetus was included in the Recommendation of the European Council no R(97)5 published in 1997. According to this Recommendation, *medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor*. For the mentioned Recommendation, see: *Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data*, (Feb. 13, 1997). <https://rm.coe.int/16806af967> (Access Date: 12.02.2019).

⁷⁷ Cranium, "Are Genetic Data of Unborn Children Subject to Data Protection Under the GDPR", <https://www.cranium.eu/genetic-data-unborn-children-subject-data-protection-gdpr/> (Access Date: 13.02.2019).

⁷⁸ Oğuzman, Seliçi and Oktay-Özdemir, p.16; If the condition of the right of capacity of the fetus is accepted as being subject to a dissolving condition, then it shall be required to accept that the child shall have the right of capacity before birth. If the fetus is not born alive or in full, then the dissolving condition shall be deemed to occur. In this case, a guardian shall be required to be appointed for the

personality shall be deemed to start as the fetus enters the mother's womb⁷⁹. However, if the fetus is not born alive, then he/she shall not have any right to capacity⁸⁰.

In cases where a person is damaged while in the mother's womb by a tortious act, then such person is entitled to demand the compensation of the damage as independent of the time between the tortious act and the formation of the damage⁸¹. The protection of personal data is accepted as a special view of the personal right⁸². If the personal data of a person is processed unlawfully when a person is in the position of a fetus, then such person is entitled to an action for compensation against the data controller, after he/she is born in compliance with the provisions of the private law⁸³. For example, procedures are required to be carried out in compliance with the provisions of LPPD when the personal data are processed while sharing the ultrasound images of a fetus in the mother's womb, processing of the information such as weight or health status.

When the legal status of the fetus while in the mother's womb is to be considered, such status shall be assumed as a part of the mother⁸⁴. Due to this reason, any intervention to the fetus constitutes an attack on the mother's personal rights. In case of unlawful processing of the fetus's personal data, the mother is entitled to action for moral and material damages due to the violation of her personal rights. This is because the medical and genetic data of the fetus are also the data concerning the health status of the mother, and accordingly, they are accepted as the personal data of the mother⁸⁵. Moreover, within this scope, they should be protected under LPPD. After the child is born, such data shall be accepted as the personal data of both the mother and the minor.

child for the abortion or the medical experiments carried out on the embryos. Serozan, *Kişiler Hukuku*, p. 422; Hüseyin Hatemi, *Kişiler Hukuku*, 6. Edition (İstanbul: Onikilevha Yayıncılık, 2017), p. 11.

⁷⁹ Tülay Aydın Ünver, *Cenin Hukuki Konumu* (Onikilevha Yayıncılık: İstanbul, 2011), p. 25. The most important purpose of this provision is to protect the fetus concerning the capacity for inheritance. This way, while the child is in the mother's womb, the fetus shall also be able to receive a share from the legacy after a live birth even if the inheritor dies. Serozan, *Kişiler Hukuku*, p. 423.

⁸⁰ For the criticism of linking the fetus's right of capacity to the dilatory condition which is to be born in full and alive (specifically for the right to life) see: Hatemi, p. 13.

⁸¹ Serozan, *Kişiler Hukuku*, p. 423.

⁸² For detailed information about this subject see: I. Section, 1.3.1. Opinion of Personal Right.

⁸³ Ünver, p. 109; Taştan, p. 33.

⁸⁴ Petek, p. 28. Oğuzman, Seliçi and Oktay-Özdemir, p. 16.

⁸⁵ Cranium, "Are Genetic Data of Unborn Children Subject to Data Protection Under the GDPR"; Taştan, p. 33.

1.1.2.4. Distinguishing the Identified or Identifiable Person

In each definition of personal data, it is not only mentioned that such data are related to one person. Moreover, it is expressed that such person is required to be identified or identifiable. For any such data to be accepted as personal data, it is required that such data directly or indirectly express such person, in other words, are required to identify such person and distinguish such person from the others⁸⁶. If the data processed directly identifies a certain person or if the data is capable of distinguishing a person from the other individuals by a simple linkage, then we can call all such data as the data relating to an identified person⁸⁷.

For a person to be called as an identifiable person, it is required that such a person can be identified by acquiring additional information other than the information acquired⁸⁸. In short, while an identified person is the person who can be distinguished in a group of identified persons, an identifiable person is the person who cannot be distinguished from the other people, but who can be distinguished with some additional information⁸⁹.

There are arguments that whether the information the data controller has shall be considered as personal data if the data subject cannot be reached with informations the data controller processing the personal data possesses, but can be identified with additional information to be obtained from another institution or person⁹⁰. According to one opinion, if the data subject can be identified by the information, sources, facilities, and technologies the data controller has, then information which the data controller has should be considered as personal data⁹¹. In other words, the data

⁸⁶ Dülger, p. 2; Başalp, *Kişisel Verilerin Korunması*, p. 33; Taştan, p. 34; Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 12.

⁸⁷ Şimşek, p. 122; Ayözger, p. 11.

⁸⁸ Çekin, *Kişisel Verilerin Korunması*, p. 37; Şimşek, p. 122.

⁸⁹ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 6.; Aksoy, p. 21.

⁹⁰ Çekin, *Kişisel Verilerin Korunması*, p. 35.

⁹¹ This opinion is commonly accepted by the German legal experts. The focal criterion here is identified as “relative criterion”. Peter Gola/ Klug Christop/ Barbara Körrfer, *Bundesdatenschutzgesetz Kommentar*, ed. Peter, Gola/ Rudolf Schomerus/ Klug Christop/ Körrfer Barbara, 12. Überarbeitete und ergänzte Auflage, C. H. Beck, 2015, P 3 Nr. 10; quoted by; Yücedağ, p. 767.

controller is required to have the potential to distinguish the identity of the data subject with the available means in order to call the available data personal data⁹².

However, the Court of Justice of the European Union adopted “objective criterion” as contrary to this decision, in its decision taken in 2016. Accordingly, if a data controller cannot identify the data subject with the available information, but is able to acquire additional information which makes such data subject identifiable, then such available information the data controller has is also considered as personal data⁹³. What is important here is to take into consideration all reasonable means which the data controller may use in order to access additional information and identify the data subject⁹⁴. In other words, if accessing the additional information is prohibited for the data controller or requires efforts non-proportional to the purpose of identifying the data subject with respect to time, cost or labor, then the available information may not be considered within the scope of personal data⁹⁵.

1.1.3. Relating to a Person

Any information directly or indirectly relates to a person is considered to be personal data⁹⁶. In other words, if the information is about any person, then that information is

⁹² In the doctrine, the opinion in which identity of the data controller and the data such data controller has is taken as the basis for the identification of the personal data is called relative identifiability. However, the type of identifiability arguing that any data used for distinguishing the data subject with any additional information irrespective of the means of the data controller is called absolute identifiability. Çekin, *Kişisel Verilerin Korunması*, p. 35.

⁹³ In this decision it was decided to determine the unlawfulness of holding the IP addresses by the Federal Republic of Germany against cyber-attacks and storage of such information for a specific period of time. In the decision, it is stated that IP address is in the nature of personal data. This is because the Federal State can apply to the prosecutor’s office and access the identity information of the data subjects. Accordingly, identifiability, which is one of the elements of the personal data, shall be realized. Court of Justice of The European Union, *Breyer v. Federal Republic of Germany*, 19.10.2016, C-582/14, Nr. 43; available at: <http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN> (Access Date: 15.02.2019)

⁹⁴ Pearce, p.318; In the Recital 26 of the General Data Protection Regulation of the European Union, it is regulated as “*to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*”.

⁹⁵ In CJEU Decision, the acceptance that IP address is a personal data since an application to a third institution can be made and the data subject can be identified by the Federal State is close to the Court of Justice’s absolute identifiability opinion. However, it does not consider the presence of such a possibility sufficient and it differs from absolute identifiability since it takes into account the conditions of not being unlawful and not requiring a non-proportional effort. CJEU, *Breyer v. Federal Republic of Germany*, 19.10.2016, C-582/14, Nr. 46.; Çekin, *Kişisel Verilerin Korunması*, p. 37; Gürsel, p. 7.

⁹⁶ Başalp, *Kişisel Verilerin Korunması*, p. 33; Taştan, p. 39.

considered as being related to such a person⁹⁷. If the information does not relate to a person, does not identify a person, then such information will not influence the privacy of the private life of a person⁹⁸. Due to this reason, such information is not protected within the frame of the personal data protection law. Data, which are not related to any person, acquired as statistical information, are called anonymous data⁹⁹.

Although the relation of information to a person is easily understandable in many cases, it shall not be that easy in some cases to determine whether it is related to a person or not. The results of a blood test in the medical file of a person, the information of a student in the automation system are explicitly related to these people.

However, to determine whether the information taken from the characteristics of an object relates to a person or not will not always be that easy. For example, the value of a house may not seem to be related to a person at first glance. The value of a property in order to determine the values of the properties in an area may not be considered as personal data at first. However, when the value of this property is used for the owner's payment of the tax liability, then it shall be considered as personal data¹⁰⁰.

The same applies to the information related to an event or process. For example, the service records to a car should not be considered as personal data since these do not relate to a person. However, determination of how many kilometers did the driver travel, or determination by the company offering the service, the frequency of the maintenances performed by the driver based on these service records make such information, information related to the driver¹⁰¹.

Following these explanations, it can be stated that; if the information reveals the identity, behaviors or characteristics of a person or if such information can be used in order to determine the behaviors or preferences of a person or to influence such person,

⁹⁷ Dülger, p. 10; Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 9.

⁹⁸ Beytar, p. 53.

⁹⁹ Başalp, *Kişisel Verilerin Korunması*, p.34; With respect to the insufficiency of the definition of personal data, and with respect to the increase of techniques, thanks to "Big Data", to relate to a person anonymous data accepted as not relating to a person, see: Pearce, p. 321.

¹⁰⁰ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 9; Dülger, p. 11.

¹⁰¹ Article 29 Data Protection Working Party, *The Concept of Personal Data*, p. 10.

then we can say that such information has the characteristic of being related to a person¹⁰².

1.2. Categories of Personal Data

In general, two types of data categories are regulated in the personal data protection law. While one of these is the personal data of special nature¹⁰³, which are protected more, have stricter conditions for processing, the other is the ordinary personal data which are excluded from the scope of the personal data of special nature.

1.2.1. Personal Data of Special Nature

According to art. 6 of LPPD, personal data of special nature relate to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data. Personal data of special nature are subjected to limited number principle¹⁰⁴ and the data to be included within the scope of personal data of special nature are listed one by one in the law¹⁰⁵. Due to this reason, the scope of the personal data of special nature cannot be expanded by interpretation¹⁰⁶.

¹⁰² Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, Brussels, 2005, p. 8. see: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf (Access Date: 25.08.2018)

¹⁰³ In this study and in LPPD these categories of data which are expressed as “personal data of special nature”, which has the potential of subjecting the persons to discrimination are regulated in GDPR as “*special categories of personal data*”, and as “*special type of personal data*” or “*sensitive personal data*” in other sources.

¹⁰⁴ Yücedağ, p. 768; Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas Kişisel Veriler ve İşlenmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Vol. LXIX, Issue.1-2 (2011), p. 319; Dülger, p. 14.

¹⁰⁵ Provision of the personal data of special nature one by one as limited number in the law is criticized by some authors. According to some of these criticisms, it is required to conditions of data processing such as the purpose of processing, the conditions of processing, the effect of the data processed on the data subject in order to determine whether the data are data of special nature. Another criticism is that whatever category the data is, it is required to examine the purpose of such processing in order to consider the data as personal data of special nature. For detailed information see: Aksoy, p. 33.

¹⁰⁶ Yücedağ, p. 768; The personal data of special nature categories are examined within a narrower scope when compared to the General Data Protection Regulation. The data categories such as “sect or other belief”, “clothing” and “membership to associations or foundations” regulated by LPPD are not regulated by GDPR. However, the reasons of lawfulness for the processing of the sensitive personal data are examined in more detail when compared to LPPD. Accordingly the data protection, which could cause discrimination of the persons and violate the fundamental rights and freedoms, were made conditional on stricter requirements.

The reason for regulating such data under a separate category is that they are data, which, if disclosed, could cause damage or discrimination for the data subject¹⁰⁷. Accordingly, personal data of special nature are protected by stricter protection in personal data protection legislation, and the processing of such data is subjected to absolute prohibition of processing¹⁰⁸. The reasons of lawfulness for the processing of ordinary personal data do not apply for the personal data of special nature. Personal data of special nature can be processed only with the explicit consent¹⁰⁹ of the data subject or in cases provided by the laws.

However, there are two categories within the personal data of special nature which are protected more when compared to the others. The data concerning the health and sexual life can only be processed without the consent of the data subject for the purpose and with the methods stated in the 3rd paragraph of the 6th article of LPPD¹¹⁰. Accordingly; *“personal data relating to health and sexual life may only be processed without seeking explicit consent of the data subject, by any person or authorized public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.”* Although the processing of such data other than for these purposes and methods is regulated by the laws, it shall be unlawful. Due to this reason, such data can be called *“strengthened personal data of special nature.”*

Although the “biometric and genetic” data regulated under the personal data of special nature category in our law are regulated as personal data of special nature in the General Data Protection Regulation, it differs with respect to the purpose of processing

¹⁰⁷ Şimşek, p. 121; Başalp, Kişisel Verilerin Korunması, p. 43. In the reasoning section of the art. 6 of LPPD this is expressed as *“The nature of the data, that is, if learned by other people, would cause the data subject to suffer or be subjected to discrimination, is taken into consideration and due to this reason, such data are considered as data of special nature (sensitive).”*, and the reason for providing a protection for such data, which is different from the other data, is stated.

¹⁰⁸ Absolute prohibition of processing means that such types of data shall not be allowed to be processed in any manner whatsoever, and if processed, shall constitute a contrariety to the law, except for the exceptions provided by the law. Özdemir, p. 127; Ayözger, p. 21.

¹⁰⁹ For detailed information about the concept of explicit consent, see: II. Section, 3.1.2.1. Explicit Consent of the Data Subject

¹¹⁰ There is also a special regulation concerning medical data in our legislation. As a result, the method for the processing of medical data is examined in more detail. R.G. No: 29863, D.20.10.2016, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, (Regulation on Processing of and Providing the Privacy of the Personal Medical Data.)

the data. While any biometric and genetic data of a person is considered as personal data of special nature in the Law no 6698, these shall be considered as personal data of special nature only if processed in order to identify the identity of a natural person in compliance with art. 9/1 of the GDPR. Accordingly, if the voice record, fingerprint or photograph of a person is processed by a special instrument, then such data should not directly be called personal data of special nature, the purpose of processing should be examined. According to the Recital 51 of GDPR, if the processing of biometric data is performed in order to determine the identity of the data subject, then these are considered as personal data of special nature. For example, if the fingerprints of the customers of a fitness center are taken by a fingerprint reading system, in order to follow the entries-exits, then these shall be considered as personal data of special nature. Whereas, the voice records of a call center processed in order to provide customer satisfaction or for burden of proof shall not be considered as personal data of special nature¹¹¹.

According to the opinion which we also agree, the fact that the expression “in order to determine the identity of a natural person” is not clearly regulated in Law no 6698 is a significant deficiency. Although not regulated accordingly in Law no 6698, if the purpose of processing the genetic and biometric data by a particular technical instrument is to identify and confirm the identity of the data subject, then it will be appropriate to consider such data as personal data of special nature¹¹². Otherwise, the image of a person taken at a store where he/she went for shopping or at a workplace shall also be considered as personal data of special nature and shall cause lawfulness reasons to be narrowed down considerably.

Determination of the personal data of special nature may not always be so easy. However, the data, even indirectly, providing access to such data should also be protected within the scope of personal data of special nature data category¹¹³. For example, if the political opinions or religious beliefs of a person can be determined from the magazines such person subscribes to, then the personal data of the data

¹¹¹ Yücedağ, p. 769.

¹¹² Yücedağ, p. 769.

¹¹³ Başalp, *Kişisel Verilerin Korunması*, p. 43; Ayözger, p. 20.

subject with respect to the magazine subscription should also be considered as personal data of special nature¹¹⁴.

1.2.2. Ordinary Personal Data

The entire personal data are important within the scope of personal data protection law without any discrimination. When data, which seem as if insignificant, are analyzed together with other data acquired or to be acquired, may become a body of information to influence the privacy of the private life and personality of the data subject¹¹⁵. Due to this reason, any information concerning a person, except the personal data of special nature, is protected within the scope of LPPD. All the general provisions contained in LPPD are related to the protection of the ordinary personal data.

1.3. Legal Nature of Personal Data

Determination of the legal nature of the personal data is essential in order to decide which legal regime to apply for the protection of such data. There are three fundamental opinions in the doctrine as personal rights, property rights, and intellectual property rights concerning which legal means and benefits such personal data protection shall serve for the protection¹¹⁶. Among these three opinions, while personal rights consider the protection of personal data more as a problem of fundamental human right, property rights and intellectual property rights consider the protection of personal rights from the economic point of view¹¹⁷.

While the personal data are examined within the scope of property rights and intellectual property rights in the Anglo-American law system, they are examined within the frame of the fundamental rights and freedoms, mainly the right to privacy¹¹⁸

¹¹⁴ Ayözger, p. 20; Özdemir, p. 27.

¹¹⁵ Şimşek, p. 121.

¹¹⁶ Aksoy, p. 38; Taştan, p. 51; Ayözger, p. 15.

¹¹⁷ Küzeci, p. 60; Taştan, p. 51.

¹¹⁸ In the Law on Protection of Personal Data no 6698, which adopted the law system of Continental Europe, also “*the protection of the fundamental rights and freedoms of people, especially the right to privacy*” is aimed. However, the right for the protection of personal data is regulated as a special right in the General Data Protection Regulation and is directly determined as “*In this Regulation....the right for protection of personal data is protected*”.

which is a special outlook of the personal rights in the law system of Continental Europe¹¹⁹.

1.3.1. The Opinion of Personal Right

Personal right defines a person's right on all the means that provide the development of the individual's self freely within the society and protection of his/her reputation¹²⁰. In other words, personal right is the right of a person on all the moral and material means that constitute the personality of a person¹²¹.

In Turkey, personal right is considered as an independent right¹²² and is protected within the scope of a general personal right in compliance with the provisions of the art. 23 and 24 of TCC¹²³. However, the some values constituting the concrete outlook of the personal rights¹²⁴ are protected by special provisions. For example, the personal rights are specifically regulated in case of violation of the personal rights under the title of the right on name in the art. 26 and 27 of TCC, or breaking of the engagement under art. 121 and due to divorce in art. 174. Moreover, the provisions for the right for compensation due to the attacks on the physical integrity of a person in the art. 56 of TCO are the provisions that protect the personality specifically.

The personal data were first considered within the scope of the right of privacy which constitutes a special outlook of personal rights in the beginning in the law system of

¹¹⁹Forde, p. 136; Kutlu ve Kahraman, p. 47.

¹²⁰ Mustafa Dural and Tufan Ögüz, *Türk Özel Hukuku-Kişiler Hukuku*, V. II, (İstanbul: Filiz Kitabevi), p. 100; Sibel Özel, *Uluslararası Alanda Medya ve İnternette Kişilik Haklarının Korunması* (Ankara: Seçkin Yayınları, 2004), p. 27.

¹²¹ Hüseyin Hatemi and Burcu Kalkan Oğuztürk, *Kişiler Hukuku* (İstanbul: Vedat Kitapçılık, 2014), p. 57; Oğuzman, Seliçi, Oktay-Özdemir, p. 172; Serap Helvacı, *Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar* (İstanbul: Beta Yayınları, 2001), p. 41; Serozan, *Kişiler Hukuku*, p. 454.

¹²² The first Civil Code in which the personal right was regulated as an independent right was the Swiss Civil Code. According to art. 28/1 of this code, "Any person whose personality rights are unlawfully infringed may petition the court for protection against all those causing the infringement". Aksoy, p. 41.

¹²³ Helvacı, *Gerçek Kişiler*, p. 103; Oğuzman, Seliçi, Oktay-Özdemir, p.205. Özel, p. 27; Osman Gökhan Antalya, *Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukuna Manevi Tazminatın İki Aşamalı Olarak Hesaplanmasına İlişkin Model Önerisi* (İstanbul: Legal Yayınları, 2017), p. 50.

¹²⁴ These values constituting the concrete, special outlook of the personal rights in application are also called "several personal rights" (*münferit kişilik hakları*) in the doctrine. Oğuzman, Seliçi and Oktay-Özdemir, p. 162.

Continental Europe and Turkey¹²⁵. The benefit protected within the personal data protection law is not the personal data itself. Upon acquiring such data, the protection of the fundamental rights and freedoms of the individual, specifically the private life is aimed¹²⁶. In Europe, the problems concerning the personal data were tried to be solved within the frame of the Right to respect for private and family life in the 8th article of the European Convention on Human Rights, before the formation of special personal data protection legislation. Moreover, it is stated in the art. 1 of LPPD that the purpose of the law is to protect the fundamental rights and freedoms of the individuals, particularly the right to privacy.

According to the opinion of the protection of personal rights, the right to privacy shall constitute an outlook of personal rights, and this will indirectly require the protection of personal data¹²⁷. Data protection rules play a supportive role in the perception and application of the right to privacy more effectively¹²⁸. Since the information related to the health, family, economic status, social and sexual preferences of the individuals are related to the private life space of such individuals, transfer and disclosure of such information to the third parties shall directly constitute interference in the private life¹²⁹. Within this frame, the violation of personal rights shall occur since the

¹²⁵ Korff, p. 4; Pamela Samuelson, "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52. Issue. 5 (1999), p. 1142; Çekin, *Kişisel Verilerin Korunması*, p. 20; For the opinion of "while the right for protection of private life is considered as a fundamental right, data protection right is a procedural right." see: Norberto Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights", *IFIP Advances in Information and Communication Technology*, AICT 352 (2011), pp. 90-107.

¹²⁶ Damla Gürpınar, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan*, Vol. 19 (Special Issue-2017), p. 684; Şimşek, p. 4; Çekin, *Kişisel Verilerin Korunması*, p. 19.

¹²⁷ Ayözger, p. 15; Aksoy, p. 55. According to an opinion discriminating the right to privacy and the data protection right, while the protection of private life is an instrument of opacity, data protection right is an instrument of transparency. Although these two concepts are distinct concepts, they also have complementary characteristics. The right to privacy performs the opacity function by preventing the intervention to private life, limiting the state's power or preventing non-proportional attacks to the private area. On the other hand, data protection law performs the transparency function by determining the rules permitting the processing of the data. For more detailed information see: Serge Gutwirth, Paul De Hert, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in E. Claes, A Duff & S. Gutwirth (eds.)", *Privacy and the criminal law*, Antwerp/ Oxford, Intersentia, 2006, pp. 61-104; Forde, p. 138.

¹²⁸ According to the author, data protection law is below the right for privacy and it plays a supportive and assistant role in the application of this right. The rules of the data protection law, which is an instrument of transparency, do not have a real value and they serve for facilitation of the protection of private life. Forde, p. 139.

¹²⁹ Oğuzman, Seliçi and Oktay-Özdemir, p. 189; Aksoy, p. 55.

procedures such as collection, recording, storage of such data have the potential to transfer such information to the third parties. Due to this reason, the protection of the personal data within the frame of personal rights shall enable the broadest scope of protection for such data¹³⁰.

Although the personal data protection right was first associated only with the right to privacy initially, its scope was extended as a result of the developing technology and the violation of human rights¹³¹. This is because the data about the person which are not private can also be protected within the scope of the personal data protection law¹³². Accordingly, the opinions basing the personal data protection only on the protection of privacy are unable to explain the protection of the personal data which are not private.

Today, the personal data protection law created a totally distinct protection area covering the protection of the free will of the individual, human dignity, freedom of belief, the right to be forgotten and freedom of thought¹³³. For example; although the data related to a person processed faultily or incorrectly result in loss of reputation of such person in the society, it does not constitute an intervention of the privacy¹³⁴. However, even in this case, the protection of personal data will become a current issue. In addition, the rights such as the correction of such faulty or incorrect data, which are

¹³⁰ Aksoy, p. 55; Ayözger, p. 15.

¹³¹ In 1983, German Constitutional Court gave a revolutionary decision with respect to the personal data protection law by its “Census” decision. Within the frame of this decision, the individuals were given the right to determine to whom and how and under which conditions such personal data can be shared. It was adjudged that the personal data processed without the consent of the individuals may harm the individual’s right to determine his/her own destiny, damage the individual’s right to develop his/her moral and material existence. Together with this decision, the personal data were freed from the narrow frame of the protection of privacy and were protected more extensively. German Konrad-Adenauer-Stiftung, *Census Act, BVerfGE 65, 1: English Translation of essential parts of the German “Volkszählungsurteil” from 15 December 1983, which established in Germany the Basic Right on Informational Self-Determination*, Honever, 11 October 2013.

¹³² Aksoy, p. 63-64.

¹³³ Şimşek, p. 119; Çekin, *Kişisel Verilerin Korunması*, p. 20; Ayözger, p. 38-52; Ayşe Nur Akıncı, “AB Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi”, *Çalışma Raporu-6* (Ankara: T.C. Kalkınma Bakanlığı, 2017), p. 32.

¹³⁴ Ayözger, p. 16.

not considered within the scope of the protection of privacy, or the right of access to any information, are granted to the data subject¹³⁵.

1.3.2. The Opinion of Property Right

The property right opinion, which constitutes the basis for the protection of personal data, is dominant more on American Law¹³⁶. According to this opinion, personal data are not only a part of personality; at the same time, they are also the products which directly arise of the person himself/herself¹³⁷. Based on this, the data subject should be given extensive legal dominance on his/her personal data and should be able to use his/her own data within the frame of the property right¹³⁸. The most important reason for this is the fact that personal data are in the focal point of the economy and accordingly, processing and sharing of data have financial benefits. As it is known, personal data are considered equal to power and became one of the most important commercial instruments of the free market economy. The enterprises process and record the data of the individuals and acquire various earnings from these data. Despite such earnings of the enterprises, the dominance area of the data subjects, who are most influenced by such processing, on their personal data is quite limited. Accordingly, due to this reason, the data subjects should be given the right to demand remuneration as a result of processing of their data¹³⁹. The data subject can file actions for compensation based on property right against and compensate his/her losses from the persons acquiring, recording or transferring his/her personal data to the third parties without the data subject's consent¹⁴⁰.

The most essential foundation of the opinion based on property right is that the persons acquiring earnings by processing and using the individuals' data are required to pay an appropriate consideration as a result of the earnings acquired from such data to the data subject who is actually influenced from this processing¹⁴¹. If the data subject

¹³⁵ This condition is limited by natural persons. This is because the legal persons are not protected by the data protection laws, and if information of such legal persons are processed, then they do not have the right to access such information. Walden ve Sawage, p. 337.

¹³⁶ Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması* (İstanbul: Beta Basım Yayın, 2014), p. 73; Aksoy, p. 57; Ayözger, p. 16.

¹³⁷ Aksoy, p. 57.

¹³⁸ Ayözger, p. 17; Aksoy, p. 57; Küzeci, p. 62.

¹³⁹ Samuelson, p. 1128; Ayözger, p. 17; Aksoy, p. 58.

¹⁴⁰ Akgül, p. 74.

¹⁴¹ Aksoy, p. 58; Samuelson, p. 1132.

possesses the personal data as in the property right, then he/she shall be free to share such data to the extent and with the enterprises he/she desires. During such sharing, the data subject shall have the power to bargain with those who desire to process the personal data concerning the consideration for such processing. This way, the data controllers shall not be able to exploit the data subjects at the end of the processing activity, the data subjects shall be stronger than their current status against the data controllers and accordingly, a balance shall be achieved between the data controllers and data subjects.

Moreover, the entities to process the personal data in consideration of a certain payment shall refrain from unnecessary personal data processing due to this reason¹⁴². Thus, this situation shall provide minimization of the disproportion between the data processing volume and the processing purpose. As a result, prevention of the violations of the human rights shall be provided. Besides, it is believed that the protection of the personal data within the scope of property right shall be more appropriate with respect to the data market. The data subjects having the right to share their data with the entities they desire, to the extent they desire, and transferring such data in consideration of a certain payment shall provide more accurate and qualified information. Accordingly, the data shall be more accurate and qualified when compared to the current state available for the data processor entities¹⁴³. Thus, the data controller or processor entities shall perform their investments within this direction and shall develop their work potentials faster.

One of the most important criticisms directed to the property right opinion is that the personal data do not comply with the property right in terms of quality¹⁴⁴. The most important reason for this is that the personal data cannot be perceived as a property on which any desired disposal can be performed. If it is perceived so, in case the data subjects share their personal data with a third party under their consent, then such third party shall be the owner of the personal data of the data subject and shall be able to transfer such data to the other parties within the direction of their desires, without

¹⁴² Samuelson, p. 1132; Aksoy, p. 59.

¹⁴³ Samuelson, p. 1133.

¹⁴⁴ Ayözger, p. 17; Aksoy, p. 64.

asking the actual data subject¹⁴⁵. This condition shall ultimately end the data subject's relation with his/her data and shall leave the data subject unprotected.

Another vital criticism directed to the property right opinion is that more loads shall be imposed both with respect to time and cost during the processing of the personal data¹⁴⁶. The those whose process personal data shall bargain with the data subjects for each data processing activity, and this shall extend the processing time and increase the cost for such processing. Moreover, it is also very complicated to determine the real costs of the personal data when selling the data of the data subjects to the third parties. Usually, the individuals sharing their data shall face problems in providing the balance between the money they will earn and the negativities they shall encounter.

1.3.3. Intellectual Property Right Opinion

The opinion that the protection of personal data depends on the intellectual property right is fundamentally based on similarities in purpose. According to this opinion, the primary purpose of protecting both the personal data and the works that are subject to the intellectual property is the protection of information and providing the control of the distribution of such information¹⁴⁷.

There may be some similarities between the personal data protection right and the moral rights of the author in the intellectual property law¹⁴⁸. The moral rights are the rights arising for the moral relationship between the author and his/her work, without any material returns¹⁴⁹. The moral rights in the intellectual property law provide rights for the author for the presentation of his/her work to the public, prevention of any changes on his/her work and determination of how, when and to whom his/her work can be transferred¹⁵⁰. When examined from this point of view, personal data protection right also provides similar rights to the data subject. The data subject has the right to

¹⁴⁵ Aksoy, p. 65.

¹⁴⁶ Samuelson, p. 1137.

¹⁴⁷ Aksoy, p. 60; Samuelson, p. 1135.

¹⁴⁸ Aksoy, p. 60; Samuelson, p. 1146.

¹⁴⁹ Ünal Tekinalp, *Fikri Mülkiyet Hukuku* (İstanbul: Vedat Kitapçılık, 2005), p. 151; Ahmet Kılıçoğlu, *Sınai Haklarla Karşılaştırmalı Fikri Haklar*, 4.Edition (Ankara: Turhan Kitabevi, 2018), p. 233.

¹⁵⁰ Kılıçoğlu, *Fikri Haklar*, p. 235; Cahit Suluk, Rauf Karasu and Temel Nal, *Fikri Mülkiyet Hukuku*, 2.Edition (Ankara: Seçkin Yayıncılık, 2018), p. 85; Emrehan İnal and Başak Baysal, *Reklam Hukuku ve Uygulaması*, (İstanbul: Onikilevha Yayıncılık, 2008), p. 145.

determine with whom and how to share his/her own data. Moreover, even if the data subject shares his/her personal data with the third parties, he/she has the right to demand prevention of changes on such data or demand the protection of the accuracy of such data¹⁵¹.

One of the essential criticisms against the opinion that bases the protection of personal data fundamentally on the intellectual property right that the values constituting the subject of both rights are different in their natures¹⁵². The works, the values such as invention and trademark that are subject to intellectual property are the products of the person's conscious work and intellectual efforts¹⁵³. However, personal data are the data which arise of the features of the individuals' personality, and which automatically occur as a result of their preferences and lives¹⁵⁴.

Moreover, the purpose of the existence of personal data protection law and intellectual property law is also different. Intellectual property law aims to develop the economy in the area of intellectual and industrial rights and to encourage the individuals to make new inventions and create works¹⁵⁵. In the societies where the intellectual property law is developed, the individuals shall be confident that their inventions and works shall be protected and shall try to create more products believing that they will acquire financial revenues from such products. However, the personal data protection law does not have such concerns. Each behavior, each preference of the individuals and each condition as a result of the individual's features shall constitute the data about such an individual. Due to this reason, it is not aimed to encourage the individuals to expose personal data in protection of the personal data. On the contrary, according to some authors, the personal data protection law limits the acquisition, usage or transfer of such data¹⁵⁶.

¹⁵¹ Aksoy, p. 61; Samuelson, p. 1148.

¹⁵² Aksoy, p. 66.

¹⁵³ Tekinalp, p. 5; Aksoy, p. 66.

¹⁵⁴ Samuelson, p.1140.

¹⁵⁵ Kılıçoğlu, *Fikri Haklar*, p. 20; Suluk, Karasu and Nal, p. 37.

¹⁵⁶ Aksoy, p.67.

2. OTHER CONCEPTS IN THE PERSONAL DATA PROTECTION LAW

2.1.Data Controller

One of the central concepts of the personal data protection law is the data controller. The data controller is the person who is mainly responsible for the unlawful processing of personal data¹⁵⁷. Upon determination of the data controller, the person who is responsible for the processing activity and who shall be addressed for the rights of the data subject stated in the law is determined¹⁵⁸. Determination of the data controller is important not only concerning the LPPD but also for determination of the civil liability, application of the criminal, and administrative sanctions. Although the general provisions shall apply for the civil liability, the determination of the unlawfulness of the data controller and the processed personal data shall be according to the provisions of LPPD.

In case of a violation concerning the personal data, it is required to examine who has the authority to decide on the issues such as *“collection of the personal data and the purpose of collection”*, *“the types of personal data collected”*, *“the purpose of use of the data collected”*, *“whose personal data shall be collected”*, *“whether the data collected shall be transferred or not, if to be transferred, to whom these shall be transferred”*, *“storage period for the data”* and *“whether the access right of the data subject or the other rights shall be applied”* in order to determine the data controller¹⁵⁹.

2.1.1. Legal Personality of the Data Controller

According to sub-paragraph(1) of the 3rd article of LPPD, the data controller *“is the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system”*¹⁶⁰.

According to this provision, the data controller can be a natural or legal person. Legal

¹⁵⁷ Brendan Van Alsenoy, “Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation”, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7, Issue.3 (2016), p. 282.

¹⁵⁸ Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of “Controller” and “Processors”*, Brussels, 2010, p. 2. see: <https://www.pdpjournals.com/docs/88016.pdf> (Access Date: 01.02.2019); Gürpınar, p. 685; Çekin, *Kişisel Verilerin Korunması*, p. 79.

¹⁵⁹ Personal Data Protection Authority, *Temel Kavramlar*, p. 24; Dülger, p. 18.

¹⁶⁰ The term *“data log holder”* is preferred in the Draft Law on Protection of Personal Data in place of the data controller.

persons are directly the data controller for the processing of the personal data and any legal responsibility to arise with respect to the relevant provisions shall directly arise in association with such legal person¹⁶¹. Within this context, general provisions shall apply for the responsibilities of the legal persons. It should be underlined here that there is no discrimination between the public sector-private sector for the persons who are responsible for the processing of personal data, both in the GDPR and LPPD¹⁶². The procedures and principles to be complied with during the protection of personal data apply to everyone.

When the personal data of the data subject are processed within the scope of the activities carried out by a legal person, the data controller shall be the legal person as a rule. However, the cases regulated by the law or the cases, in which the legal person explicitly, without any room for doubt, appoints a person as the data controller, are the exceptions of this condition. This is because the qualification of a legal person as the data controller shall provide stronger and more stable protection for the data subject with respect to the data protection rights¹⁶³.

The personal data processed by the persons working within the structure of the legal person or acting on behalf of the company, within the scope of the company activities are considered as the action of directly the legal person in terms of civil liability¹⁶⁴. The legal person shall be responsible if any liability arises as a result of such activities. However, if the person acting on behalf of the company processes the data of another person for his/her own purposes, outside the control and field of activity of the legal person but with the means of the legal person during processing such data, then such

¹⁶¹ Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, Ankara, 2017, p.1. see: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf> (Access Date: 10.10.2018)

¹⁶² Dülger, p. 19; Kutlu and Kahraman, p. 46; Çekin, *Kişisel Verilerin Korunması*, p. 41; Başalp, *Kişisel Verilerin Korunması*, p. 35.

¹⁶³ Article 29 Data Protection Working Party, *The Concepts of "Controller" and "Processors"*, p. 16.

¹⁶⁴ The legal person is also directly responsible for the personal data processed by the units such as human resources, administrative affairs, information processing within the structure of the legal persons. This is because these units do not have a personality which is independent of the legal person. However, since each company contained within the structure of a holding has an independent legal personality, each one of these companies has the quality of an independent data controller. Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p. 1; Dülger, p. 18.

natural person data controller is considered to be responsible for such processing activity. He/she shall be responsible for the damage to arise as a result.

In this case, the legal person should be held responsible within the scope of both the employer's liability and the performance assistant with respect to the civil liability based on the case in question. Such responsibility continues within the scope of LPPD due to not taking the required security measures¹⁶⁵.

2.1.2. Determination of the Purposes and Means of Personal Data Processing

The most important characteristic of the data controller that distinguishes him/her from the other personal data processing actors is that the data controller determines the purposes and means of personal data processing¹⁶⁶. In other words, whoever determines the answers to the questions of "why" and "how", that person is the data controller¹⁶⁷. Accordingly, the data controller is not under any liability for holding such personal data; the actual liability arises from the determination of the purposes and means of the processing of such data.

For example, a bank shall be considered as the data controller in case processing and retaining the account data of the customers. This is because the person determining the manner of usage of the data together with the purpose and means of processing such data are is the bank legal person. However, if the bank transfers such data to a software company for more systematic and safer processing, the mentioned software company holding such information shall not be the data controller. The reason for this is that such data are kept for the bank legal person, which is the data controller. The software company shall act according to the instructions of the data controller, which is the bank legal person, with respect to the issues such which personal data shall be processed for which purposes, how such data shall be stored and processed, who shall have access to such data and when such data shall be erased¹⁶⁸.

¹⁶⁵ Article 29 Data Protection Working Party, *"The Concepts of "Controller" and "Processors"*, p. 16.

¹⁶⁶ Article 29 Data Protection Working Party, *"The Concepts of "Controller" and "Processors"*, p. 13; Leyla Keser Berber, *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması* (İstanbul: Onikilevha Yayıncılık, 2014), p. 32.

¹⁶⁷ Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p. 3.

¹⁶⁸ Article 29 Data Protection Working Party, *The Concepts of "Controller" and "Processors"*, p. 14.

However, it is possible for the data processor to exclusively determine the technical and organizational data processing means under a data processing contract.¹⁶⁹ The reason for this is that the data controller transfers the data processing activity to the data processor since these people have expertise in this field.¹⁷⁰ However, the data controller should be notified in full about the utilization of these means which are used in order to realize the purpose of data processing¹⁷¹.

In compliance with the explanations given above, the person determining the purpose of the processing of the personal data shall be the data controller under any condition. However, the determination of the means used for the realization of the purpose can be transferred by the data controller to the data processor in cases where there are technical and organizational problems¹⁷².

2.1.3. Joint Data Controllers

In compliance with art. 26 of GDPR, in cases “*where two or more data controllers jointly determine the purposes and means of processing,*”, such data controllers shall be joint data controllers. Joint data controller is not clearly regulated in LPPD. However, the joint data controller concept is essential both in the practice and EU sources.

The most important thing about joint data controlling is that the data controllers determine the purposes and means of processing equally and due to this reason, they are responsible for such processing equally. However, this is only one type of having more than one data controllers. More actors can be determinant at various stages of processing activities during the processing of personal data. Accordingly, determining the joint data controllers is harder and more complicated than it seems.

¹⁶⁹ Çekin, *Kişisel Verilerin Korunması*, p. 80; Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors”*, p. 17.

¹⁷⁰ The data controller may authorize the data processor in issues such as; “*which information technology systems or the other methods shall be used for the collection of personal data, the method for storage of such data, the details of the security measures to be taken for the protection, which method shall be used for transfer, the method to be used for the correct application of the terms related to the storage, the methods for the erasure, destruction and anonymizing*”. Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p.4.

¹⁷¹ Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors*, p.14.

¹⁷² Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors”*, p.15.

The joint data controllers may sometimes have very close relations during the processing activities and may share the roles and responsibilities equally. The cases where all the processing purposes and means are determined jointly during the processing of the personal data can be given as an example. However, this relation between them is sometimes very weak. For example, they may only have the same data processing purposes but different means or vice versa. Even in some cases, the purpose of processing and means can be completely different, but there can be joint data controllers. Due to this reason, joint data controlling may be in various forms in the application.

Determination of the roles and responsibilities of the joint data controllers during the processing activities is important for determining the level of responsibilities for the personal data violations to occur. However, it is not possible to categorize or classify these due to the plurality of joint controlling cases. First of all, it is required that they should satisfy the condition of being the general data control in determination of the joint data controllers. While the joint data controllers decide the purpose and means of processing together in some cases, they decide the purpose together and differ in the means of processing in other cases. Alternatively, while one data controller performs a part of the processing activities, the other data controller performs another stage. However, there should be integrity when such processing activity is considered as a whole.

The contract between the parties is required to be examined when the roles and responsibilities of the joint data controllers are to be assessed. However, the state in the contract may not always reflect the actual status. Due to this reason, the decision should be given after examining the concrete factors such as the purpose of the processing, independence and the means used by the parties during the processing activity. In other words, although it is stated in the contract that one party performs activities as the data processor for the other party, both parties acquire the title of the joint data controller in cases where they determine the purpose or the basic factors for the means of data processing for the whole or a part of the processing activity.

For example, a pharmaceutical company signs a contract with a research company in order to measure customer satisfaction. The research company independently carries

out the selection of the respondents of the questionnaire, method, and scope of the questionnaire¹⁷³. In this case, the research company, although it processes the data in favor of the pharmaceutical company, shall qualify as the joint data controller since it is independent to the issues such as the decision on whose data to collect and how to process.

2.2.Data Processor

The natural or legal person processing the data on behalf of the data controller and as based on the authorization provided by the data controller is called data processor in Personal Data Protection Law¹⁷⁴. Although, there is processing authorization for the personal data as based on the authorization given by the data controller, the person to decide on the outcome of such data is the data controller¹⁷⁵.

As it can be understood from the definition of the data processor, a person performing data processing two factors should be examined in order to determine that a person performing the processing activity is the data processor. The first one is that the person processing the data is required to be a separate legal person outside the organization of the data controller¹⁷⁶. Due to this reason, the employee of the legal person processing the data on behalf of the legal person shall not have the title of the data processor. This is because this person is the person mediating for the reflection of the will of the legal person acting as the data controller. In other words, the activities carried out as the authorized organ of the legal person within the scope of the activities of the legal person shall be considered as the activity of such legal person.

The most important factor in determining a person as the data processor in a personal data processing activity is the acting of such person on behalf of the data controller when performing the processing activity. The data processor is required to comply with the instructions of the data controller while processing the personal data. The data processor does not have any discretionary power in determining the purpose of and the

¹⁷³ Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p. 5.

¹⁷⁴ The data controller authorizes the data processor for processing the personal data by concluding a *personal data processing contract*. Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p. 1.

¹⁷⁵ Çekin, *Kişisel Verilerin Korunması*, p.79; Berber, p. 33.

¹⁷⁶ Personal Data Protection Authority, *Veri Sorumlusu ve Veri İşleyen*, p. 1; Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors”*, p. 25.

basic means used for processing of the personal data. What is meant by basic means is the means that directly affect the legality of personal data processing. For example, the data controller determines the issues such as which data to process, the time for storage of such data or who can access such data¹⁷⁷. Accordingly, the data processor is required to comply with the instructions of the data controller. The person acting in a manner to exceed the mentioned authorities, who is authorized in the determination of the purpose of data processing or the basic means of data processing is considered to act as the joint data controller¹⁷⁸.

2.3.The Concept of Processing of Personal Data

Defining the concept of processing of personal data is essential in order to determine which types of activities on personal data shall be considered within the scope of the protection of personal data. The concept of processing of personal data is the series of operations that are carried out on personal data such as collection, recording, storage, alteration, re-organization, or preventing the use thereof¹⁷⁹.

Any operation in which the personal data are processed by automatic means¹⁸⁰ shall be handled within the scope of LPPD¹⁸¹. The distinction between automatic or semi-automatic processing stated in the law is determined based on whether or not there is human interference during the data processing¹⁸². In other words, if the personal data processing is performed, processed or transferred to the third parties automatically by automatic means without any human interference, then this is called full automatic

¹⁷⁷ Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors”*, p. 32.

¹⁷⁸ Article 29 Data Protection Working Party, *The Concepts of “Controller” and “Processors”*, p. 25.

¹⁷⁹ Ayözger, p. 131; Özdemir, p. 135; Küzeci, p. 327; Personal Data Protection Authority, *Temel Kavramlar*, p. 15; Çekin, *Kişisel Verilerin Korunması*, p. 38. In art. 3/1(e) of the LPPD processing of personal data is regulated as “any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means”.

¹⁸⁰ If computer or similar automation systems are used for the processing of personal data, then such data shall be considered as processed automatically. See: Başalp, *Kişisel Verilerin Korunması*, p. 32; Taştan, p. 43. According to Küzeci what should be understood from automatic processing is all the processing activities in which technical support is provided other than the manual data. Küzeci, p. 328; According to another definition; it is the processing activity carried out by the devices with processors such as computers, telephones, watches etc., automatically by the pre-prepared algorithms via the software and hardware features, without human interference. see: Personal Data Protection Authority, *Temel Kavramlar*, p. 18.

¹⁸¹ Başalp, *Kişisel Verilerin Korunması*, p. 32; Taştan, p. 43.

¹⁸² Çekin, *Kişisel Verilerin Korunması*, p. 22; Dülger, p. 16.

processing. For example, the smartphones' processing of the users' data or the search engines' processing of the individuals' behaviors on the internet can be considered as full automatic systems. However, if the processing of the data is provided by a person, and these devices are being used as an instrument, then semi-automatic processing takes place. For example, registering the customer data on the banking system by a bank employee, via computers is semi-automatic processing. These two processing methods, regardless of whether they are included within a data registry system or not, are protected under LPPD.

However, as it can be understood from the definition of processing, it is not compulsory to process the data only with automatic means for the personal data to be protected within the scope of LPPD. The data processed by non-automatic means shall also be protected within the frame of LPPD. However, there is a condition for the protection of data within the scope of the law if data is processed via non-automatic means. Accordingly, the data is protected only if processed *as a part of data registry system*¹⁸³. For example, if a lawyer processes the case list and case subjects of his/her client in a manual file in a chronologic order or by different criteria, then this activity shall also be included within the scope of LPPD.

2.4.Data Registry System

According to art. 3/1(h) of LPPD, "*data registry system is the registry system which the personal data is registered into through being structured according to certain criteria*"¹⁸⁴. The concept which was regulated as data log in the previous draft was then changed as data registry system. This system can be created physically as well as over electronic or digital medium. For the protection of the personal data processed through non-automatic means within the frame of LPPD, such data are required to be a part of the data registry system. However, if the mentioned data are not a part of a data registry system but have the quality of being personal data, and if damage arises as a result of unlawful activities concerning such data, then the liability provisions within the scope of Turkish Civil Code and Turkish Code of Obligations apply. The

¹⁸³ Dülger, p. 16; Çekin, *Kişisel Verilerin Korunması*, p. 23; Taştan, p. 44.

¹⁸⁴ Ayşe Nur Akıncı, p. 11; Dülger, p. 17.

unlawful activities concerning such data shall be considered as crime in compliance with Turkish Penal Code¹⁸⁵.

3. FUNDAMENTAL PRINCIPLES IN DATA PROTECTION LAW

Certain minimum principles are determined since the first legal regulations in personal data protection law and this law branch was developed within the direction of these principles. Although there are differences in the approaches in many international regulations, it can be stated that some fundamental principles are common in all the regulations¹⁸⁶.

One point should be underlined before examining these principles during the processing of personal data one by one. It is very complicated, almost impossible to separate these principles from each other by a definite line. This is because these principles are connected, interlocked, and complete each other¹⁸⁷. In some cases, the processing carried out with the lack of a principle may cause another principle to be violated. Due to this reason, when examining these principles below one by one, we should also take the relation between them into account.

These principles stated in LPPD shall be applied for any types of processing activities¹⁸⁸. Any processing performed against these principles shall cause the processing of personal data to be unlawful¹⁸⁹. Even if the data controller performed processing in compliance with the provisions regulated by the art. 5 to 9 of the LPPD, in case the processing of the data constitutes non-conformity to these principles, then it shall be unlawful. In other words, processing in compliance with the principles in the 4th article may not always be lawful. The other lawfulness requirements in the other articles of the LPPD are also required to be fulfilled. However, any processing that is contrary to the 4th article shall be unlawful.

¹⁸⁵ LPPD Preamble, p. 7.

¹⁸⁶ GDPR, art. 5; EU Directive no 95/46/EC, art. 6; EC Data Protection Agreement, art. 5; UN Guidelines 1. Principle; OECD Guidelines par. 7.

¹⁸⁷ Küzeci, p. 205.

¹⁸⁸ Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*, Ankara, 2017, p. 41; Dülger, p. 107.

¹⁸⁹ Çekin, *Kişisel Verilerin Korunması*, p. 42.

According to the LPPD, the first requirement for the processing of personal data is that any processing activity for such data should have a legal basis. This principle is stated in the art. 4/1 of LPPD as “*Personal data may only be processed in compliance with the procedures and principles set forth in this Law and other laws*”. As it could be understood from this provision, processing of the personal data is prohibited as a rule¹⁹⁰. However, if the processing has legal basis, then it may be performed lawfully.

EU and Turkey, which handle the protection of personal data with the approach of the protection of human rights, took a step with this regulation parallel to the principle of limitation of the fundamental rights and freedoms only by laws¹⁹¹. In addition to this, 3rd paragraph of the art. 20 of the Constitution concerning the personal data, it is set forth that the personal data can only be processed as provided by the law or with the explicit consent of the individual.

The basic principles for the processing of personal data are regulated in art. 4/2 of LPPD¹⁹². These principles are (i) *lawfulness and conformity with rules of bona fides*, (ii) *accuracy and being up to date, where necessary*, (iii) *being processed for specific, explicit and legitimate purposes*, (iv) *being relevant with, limited to and proportionate to the purposes for which they are processed*, (v) *being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed*.

3.1.Lawfulness and Conformity with Rules of Bona Fides

One of the key principles of the personal data, for which consensus is achieved in many international regulations, is the principle of lawfulness and conformity with rules of bona fides¹⁹³. It should be stated that this principle covers all other principles with respect to the processing of personal data and constitutes the basis for such principles¹⁹⁴. During the examination of this principle, we believe it shall be more

¹⁹⁰ Çekin, *Kişisel Verilerin Korunması*, p. 42.

¹⁹¹ According to the art. 13 of the Constitution of Turkish Republic “*Fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence.*”

¹⁹² These principles in our Law are mainly regulated by taking into account convention no 108 and Directive no 95/46EC. Personal Data Protection Authority, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, Ankara, 2017, p. 1.

¹⁹³ Art. 4/2(a) of the LPPD; art. 6/1 of DPD no 95/46/EC, art. 5/1, (a) of GDPR.

¹⁹⁴ Küzeci, p. 206; Ayözger, p. 134; Ayşe Nur Akıncı, p. 32. According to GDPR compliance of the data controller with the laws and rules of bona fides is not sufficient, the principle of transparency is

beneficial to examine the concepts of lawfulness and conformity with rules of bona fides separately in order to understand the subject better.

3.1.1. Lawfulness

The requirement for the lawful processing of personal data means the obligation of not acting contrary to the provisions imposed by the laws and other legal legislations while processing such data. Accordingly, action should be taken in compliance with the legal requirements concerning the processing of data in the LPPD and other legal regulations during the processing of the personal data. Based on this, contrariety to the other principles of the law shall directly be considered as contrariety to the lawfulness.

However, stipulation of data processing by the provisions of the law does not make such data processing lawful.¹⁹⁵ In addition, such provision should be regulated in compliance with the general provisions of the Constitution and the 13th article concerning the restriction of the fundamental rights and freedoms. This is because each data processing activity has the nature of interfering the individual's fundamental rights and freedoms. Each personal data processing activity based on a law which does not match up with the Constitution shall mean the violation of the fundamental rights and freedoms of the individuals.

3.1.2. Conformity with Rules of Bona Fides

The data controller is required to act in compliance with the rules of bona fides while processing personal data. Since the determination of the limits of acting in compliance with the rules of bona fides is an abstract concept, it is more difficult when compared to the principle of lawfulness. The rule of bona fides means the behaviors which are expected of an honorable, honest person¹⁹⁶. For the protection of the personal data, it is required that the data controller complies with the rules of bona fides, and protects the interests of the data subject and satisfy the reasonable expectations during the

also required to be complied with. Accordingly, a very strict responsibility is imposed on the data controller. European Data Protection Supervisor, *The Data Protection Reform Package*, p. 19.

¹⁹⁵ Dülger, p. 110.

¹⁹⁶ M.Kemal Oğuzman and Nami Barlas, *Medeni Hukuk Giriş, Kaynaklar, Temel Kavramlar*, 24.Edition (İstanbul: Vedat Kitapçılık, 2018), p. 222.

fulfillment of the purpose of the data processing¹⁹⁷. In compliance with the rule of bona fides, the data controller should process the personal data in a transparent manner¹⁹⁸ and should notify the data subject at each stage of the processing and take the required measures with respect to the rights and liabilities.

3.2. Accuracy and Being Up To Date Where Necessary

The data subject has the right to demand the accurate processing of his/her data or updating of the data which are not up to date. Due to this reason, the data subject has the right to access such personal data during the processing stage and may request the erasure or correction of the faulty or outdated data¹⁹⁹. What should be taken into account according to the principle is that the personal data should absolutely be kept accurate, and the data processed inaccurately should definitely be corrected or erased²⁰⁰. However, the correction of the outdated personal data which were accurately processed is required, “*where necessary.*”²⁰¹ Due to this reason, outdated data, for which the data subject does not have requests or of which it is understood that the data processing purpose shall not be achieved in case not updated or similar reasons, are required to be amended, erased or destroyed.

The right of the data subject regulated by the art. 11/1(d) of the LPPD, to request the rectification of the incomplete or inaccurate data, if any, is the concrete outlook of this principle. Accordingly, the data controller is required to take the measures for the accuracy and up-to-dateness of such information.

¹⁹⁷ Küzeci, p. 207; Çekin, *Kişisel Verilerin Korunması*, p. 45; Due to this reason, should not perform the processing activities which the data subject cannot stipulate and should take all the administrative and technical measures required in order to prevent the occurrence of the consequences which the data subject cannot predict. Dülger, p. 111.

¹⁹⁸ Dülger, p. 112; Özdemir, p. 137.

¹⁹⁹ Şimşek, p. 100; Özdemir, p. 145; Ayözger, p. 145;

²⁰⁰ Determination of the correctness of data is only possible by taking the concrete data as the basis. Due to this reason, the data obtained as a result of any thoughts or as a result of subjective evaluations shall not constitute the violation of the accuracy principle, no matter how faulty or meaningless they are. Dülger, p. 130.

²⁰¹ Dülger, p. 130.

3.3. Being Processed for Specific, Explicit and Legitimate Purposes

During the processing of personal data, the whole processing should be carried out with specific, explicit and legitimate purposes²⁰². This is because the data subject, who does not clearly know the purpose of processing the personal data, cannot make a correct decision for providing his/her consent for the processing of the data and loses his/her dominance over his/her data²⁰³. Thanks to this principle, the limits of the purpose of processing the personal data shall clearly be defined, and such data shall be required to be used only within the direction of such purpose²⁰⁴. However, the specificity of the purpose is not sufficient by itself. It is also required for such purpose of being legitimate.

According to this principle, the data controller should clearly determine the data processing purpose before the processing activity and should notify both the data subject and the national inspection unit. Due to this reason, the data controller holding the personal data of the data subject should not use such data for unspecific, uncertain or open-ended purposes. Storage or acquisition of any data for future use without anonymization or destruction shall constitute contrariety to this principle²⁰⁵. During the processing of personal data, the prohibition of processing the personal data for unspecific purpose and for the probability of use within the direction of a potential purpose to occur in future is the result of this principle²⁰⁶. Thanks to this principle, the data subject has the right to learn the purpose for acquisition of such data from the institutions and organizations processing such personal data, and whether or not they are processed for the mentioned purpose²⁰⁷.

Again according to this principle, the purpose of processing the personal data should be legitimate. For the legitimacy of the purpose of processing the personal data, the

²⁰² Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, Brussels, 2013, p. 15. see: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Access Date: 10.10.2018)

²⁰³ Küzeci, p. 213; Çekin, *Kişisel Verilerin Korunması*, p. 46.

²⁰⁴ Şimşek, p. 84.

²⁰⁵ Başalp, *Kişisel Verilerin Korunması*, p.37; Küzeci, p.209; Çekin, *Kişisel Verilerin Korunması*, p.46.

²⁰⁶ Özdemir, p.142; Osman Şahin, *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması, Bilgi Teknolojileri ve İletişim Kurumu*, (Ankara, 2011), p.73; Ayözger, p.138.

²⁰⁷ Ayözger, s.138; Başalp, *Kişisel Verilerin Korunması*, s.38; Şimşek, s.83.

criteria such as processing as based on a legal foundation, being in compliance with all the legal requirements and the balance between the benefit to be acquired from processing the data and the volume of data to be processed should be taken into consideration²⁰⁸. The cases concerning the legitimacy of the purpose, which we shall examine in detail in the lawfulness reasons below, are regulated in the articles 5 and 6 of the LPPD and articles 6 to 10 of the GDPR.

Finally, the data controller, even if the personal data are acquired within the frame of a specific and legitimate purpose, is required to act in compliance with this purpose during the following processing activities²⁰⁹. If the purpose of processing the personal data changes afterward, the data controller is required to get the consent of the data subject again, or the lawfulness requirements stated in the LPPD are required to exist²¹⁰. The most important reason for this is that a person processing the personal data once as based on legitimate and specific purpose uses such data afterward as independent of these purposes and takes the data subject's dominance on such data²¹¹. In other words, this state shall be contrary to the right to determine the future of the information constituting the source of the protection of the personal data. For example, where the contact information of the parents is processed in a private teaching institution in order to reach the parents of the students in case of an emergency, sending notification messages concerning advertising and marketing to such contact numbers afterwards will constitute contrariety to this principle.

However, in some cases, it may be required for the new purposes emerging later to comply with the previous purpose or to complete such purpose. In this case, if the data

²⁰⁸ Küzeci, p.199; Akgül, p.128; Ayözger, p.139. *Akıncı*, defined the legitimacy of the purpose as the requirement and connection of the personal data processed to the work performed or the service rendered. Ayşe Nur Akıncı, p.32; According to *Dülger*, the presence of only legal basis is not sufficient for the legitimacy of a processing, it also requires to be in compliance with the objective social values within the scope of the principle of bona fides. *Dülger*, p.120.

²⁰⁹ Başalp, *Kişisel Verilerin Korunması*, p.39; European Data Protection Supervisor, *The Data Protection Reform Package*, p. 20.

²¹⁰ This state is expressed in the preamble of the LPPD as “for processing data in order to satisfy the potential needs to occur later, one of the requirements for the personal data processing regulated by the 5th article is required to take place as if the processing is started for the first time.”. Özdemir, p. 141; Ayözger, p. 138; Çekin, *Kişisel Verilerin Korunması*, p. 48.

²¹¹ Küzeci, p. 212.

controller or the processor processes the personal data in a manner to comply with the rules of bona fides, then there will be no violation²¹².

3.4. Being Relevant with, Limited to and Proportionate to the Purposes for Which They Are Processed

According to this principle, the data controllers are required to process the minimum data possible in order to achieve the purpose. Accordingly, processing of the personal data for the purposes other than the processing purpose, as irrelevant with the purpose or processing of data which is unnecessary for the realization of the purpose shall constitute contrariety to this principle²¹³.

Within the frame of this principle, the data controller should determine whether or not there is another alternative for achieving the purpose, other than processing personal data. If such purpose can be achieved in another way, then the data controller should prefer that way first²¹⁴. However, if data processing activity is required for such purpose, then the data controller should process the minimum personal data possible in order to achieve such purpose²¹⁵. This way, the processing of the personal data which are not required to be processed during data processing activity is tried to be prevented. For example, the employer should ask for information appropriate for the quality of the work and work conditions from the candidate during an employment application. If the employer demands information more than the work relation requires, then the employer shall violate the principle of proportionality.

In compliance with the principle of proportionality in the processing of personal data, it should be examined in processing of each data whether this is in compliance with the processing purpose and whether this is required for achieving the purpose²¹⁶. As a result of the examination carried out on the basis of a concrete case, the issues such as

²¹² Ayözger, p. 138; Although this is not mentioned in the LPPD, it is regulated in the 4th paragraph of the 6th article of GDPR. According to the Regulation, if the data controller shall use the personal data for a purpose other than the purpose for which such data were collected, then such purpose should be compatible with the collection purpose.

²¹³ European Data Protection Supervisor, *The Data Protection Reform Package*, p. 20; Ayözger, p. 140; Başalp, *Kişisel Verilerin Korunması*, p. 38; Dülger, p. 124.

²¹⁴ Küzeci, p. 214; Çekin, *Kişisel Verilerin Korunması*, p. 53.

²¹⁵ This approach is called “data economy” in the doctrine. Moreover, this principle is called “data minimization” in the doctrine. Dülger, p. 124.

²¹⁶ Özdemir, p. 143; Ayözger, p. 141; Şimşek, p. 125.

whether there is a change in the purpose during the collection of data and the purpose after processing, the benefits of the expectations of the data subject, the nature of the personal data, its impact on the data subject following the processing or the medium in which such data are processed should be taken into consideration²¹⁷.

3.5. Being Retained for the Period of Time Required

The data processed should be retained for the period of time stated in the relevant legislation in compliance with art. 4/2 of LPPD or for the period of time that applies for the purpose for which these are processed. By the end of such periods, the such data should not be retained anymore, they should either be anonymized or erased and destroyed²¹⁸. These procedures may seem easy at first glance, but it is a very complex process for a data controller, who has multiple systems, to classify and follow up the level and time of erasure of the data subject's data and from which system and when such data shall be erased²¹⁹.

This principle is an outlook of the *right to be forgotten*²²⁰ which is regulated in the 17th article of GDPR. This right is mentioned in a decision of the Court of Justice of the European Union (CJEU) dated 2014²²¹. This is a case filed by a Spanish lawyer with respect to the data concerning the sale of a property made 16 years ago, which was not erased by the Google's operators, although such erasure was explicitly requested by the data subject. Following the decision of the Spanish courts that the company should erase the data subject's data, the case was referred to CJEU after the court of appeals. The Court of Justice adjudged that the data which became irrelevant later or which do not have any benefit for the public should be erased upon the demand of the data subject or *ex officio* in compliance with the provisions of the Directive no 95/46/EC²²².

²¹⁷ Article 29 Working Party, *Purpose Limitation*, p. 23-26.

²¹⁸ Başalp, *Kişisel Verilerin Korunması*, p. 39; Şimşek, p. 84-85; Ayözger, p. 144; Özdemir, p. 143-144.

²¹⁹ Ayşe Nur Akıncı, p. 15.

²²⁰ For detailed information about the right to be forgotten see: Sabire Sanem Yılmaz, *Kişisel Verilerin Korunması Regülasyonu ve Unutulma Hakkı*, İstanbul Barosu Dergisi, Volume. 92, No:5, 2018, p. 188-193; European Data Protection Supervisor, *A comprehensive approach on personal data protection in the European Union*, Brussels, 2011, s. 18; Berber, p. 67; Eren Sözüer, *Unutulma Hakkı- İnsan Hakları Hukuku Perspektifinden Bir İnceleme* (İstanbul: Onikilevha Yayıncılık, 2017).

²²¹ CJEU, *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, 13.05.2014, *Case C-131/12*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN> (Access Date: 17.02. 2019)

²²² Kutlu and Kahraman, p. 48.

For example, according to art. 5 of the Directive no 2002/58/EC the data called “*traffic data*” in electronic communication sector, which are processed in order to enable communication, should be erased or should be anonymized following the termination of the communication. However, the traffic data required for billing and interconnection can be processed. Such data and billing can be objected legally or can be kept for the duration in which the payment can be followed²²³.

Another CJEU decision concerning the erasure or destruction of the personal data, which is important for EU, is the *Digital Rights Ireland Decision*²²⁴. According to this decision, it is accepted that the processing and storage of the data related to the individuals’ fixed line, mobile line internet telephone calls over electronic communication services and public communication networks or e-mails, without any legal grounds is unlawful. Due to this reason, the Directive no 2006/24/EC²²⁵ was abolished.

Finally it should be stated that, when making an application for registration in cases where the data controller is required to enroll the Registry of Data Controller in compliance with the art. 16 of the LPPD, data controller should also notify the maximum time required for the purpose for which the personal data are processed²²⁶.

3.6.Accountability

With a new provision added to art. 5/2 of the GDPR, it is regulated that the data controller is responsible for acting in compliance with the general principles and that

²²³ Yıldız, p. 799. There is an provision concerning this in the art. 5/17 of the Electronic Communication Law no 5809. According to this provision “*Traffic data are processed only by the personas authorized by the operator for the purposes of traffic management, interconnection, billing, determination of irregularities and frauds and similar transactions or for the settlement of disputes including the customer complaints and interconnection and billing disagreements*” For the relevant law see: No:5809, Adoption D. 05.11.2008, O.G.No: 27050, D.10.11.2008.

²²⁴ CJEU, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, ve Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others cases*, 08.04.2014, ECR-(2014) I-238, see: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN> (Access Date: 10.12.2018).

²²⁵ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. see: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063: EN:PDF> (Access Date: 03.11.2018).

²²⁶ LPPD Preamble, p. 8.

he/she is required to demonstrate such compliance with the Regulation²²⁷. This principle is called the principle of accountability. The principle of accountability imposes two different responsibilities on the data controller. The first one is that the data controller shall be responsible for the consequences of the actions which do not comply with the principles in the Regulation. The data controller shall be responsible in person for the damages to arise as a result of unlawful processing of the personal data.

Another responsibility imposed on the data controller is the demonstration of the compliance of his/her actions with the Regulation. Contrary to the general provisions²²⁸ the data subject claiming that the personal data are unlawful is not under the obligation to prove the unlawfulness of this. On the contrary, the data controller is required to prove that he/she processed the personal data in compliance with the Regulation in order to be relieved from this responsibility. The most important innovation brought by this provision is that the data controller and in some cases, the data processor is required to prove clearly that he/she acts in compliance with this Regulation²²⁹. Although some provisions of the Directive 95/46/EC also impose responsibilities on the data controller for proving that he/she lawfully processes the personal data, the Regulation have clearly regulated this issue.

In Turkish law, although the accountability obligation of the data controller is not clearly stated as in the Regulation, the provisions in art. 10 of LPPD arranging the data controller's obligation to inform the data subject, and in art. 11 of LPPD arranging the data subject's rights to be notified about whether or not his/her personal data are processed, and if processed than to request information about this processing, about the purpose of processing and whether or not they are used in compliance with this purpose, impose an obligation on the data controller for accounting. Moreover, the data subject's right to demand compensation in compliance with the general provisions from the data controller with respect to the damage incurred by the data subject as a

²²⁷ European Data Protection Supervisor, *The Data Protection Reform Package*, p. 120; Çekin, *Kişisel Verilerin Korunması*, p.12; Alsenoy, 282.

²²⁸ According to the general provisions, the claimant is required to prove his/her claim. This state is expressed as “*Unless otherwise provided in the Code, any one of the parties has to prove he facts on which his/her/its claim is based*” in the art. 6 of Turkish Civil Code. As it can be understood from this provision, this provision, although is a general rule, has exceptions.

²²⁹ Korff, p.1.

result of unlawful processing of the data, regulated in the articles 11 and 14, regulation of administrative fines are the provisions that regulate the legal responsibility of the data controller.

SECTION II

THE BASIS FOR THE CIVIL LIABILITY OF THE DATA CONTROLLER

1. THE CONCEPT OF CIVIL LIABILITY

Liability²³⁰, is the individual's assumption of the results of his/her own behaviors or any event taking place in his/her area of dominance. In other words, it is the obligation of compensating the damages suffered as a result²³¹. The concept of liability is used in two different ways in the doctrine. While the first one studies “*with what*” such individual is held liable, the other one studies “*why*” such individual shall be held liable. Due to this the first definition is called “*liability with...*” and the other is called “*liability from...*”²³².

“*liability with...*”, is when the debtor is liable to the creditor with his/her properties for the fulfillment of the obligation²³³. Although the right to claim entitles the creditor with the authority to demand, the creditor shall lack legal protection by the end of this demand in the rule of law, in case there are no means forcing the debtor to fulfill the

²³⁰ With respect to legal relations, the concept of liability is used in different meanings in various areas. Political liability constitutes the politicians' liability against the public, criminal liability constitutes the liability of the individuals to occur as a result of non-compliance with the rules of criminal law. Erol Cansel and Çağlar Özel, *Borçlar Hukuku Genel Hükümler*, Vol. I, 2.Edition (Ankara: Seçkin Yayıncılık, 2017), p. 83. We shall examine legal liability in this study.

²³¹ Türk Dil Kurumu, *Güncel Türkçe Sözlük*, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c753d5730b0a0.29668248 (Access Date: 07.09.2018).

²³² Fikret Eren, *Borçlar Hukuku Genel Hükümler*, 23. Edition (Ankara: Yetkin Yayınları, 2018), p. 510; Ahmet Kılıçoğlu, *Borçlar Hukuku: Genel Hükümler*, 21.Edition (Ankara: Turhan Kitabevi, 2017) p. 45.

²³³ M. Kemal Oğuzman and Turgut Öz, *Borçlar Hukuku Genel Hükümler*, Vol. I, 16.Edition (İstanbul: Vedat Kitapçılık, 2018), p. 16; Eren, p. 510.

obligation. Due to this reason, the factor of liability has arisen in the current rule of law in order to protect the creditor and to provide the debtor to fulfill the obligation. “*liability with...*” entitles the creditor to force the debtor, who does not fulfill his/her obligations, through the government authorities or to confiscate the properties of the debtor²³⁴. The debtor guarantees the creditor, the fulfillment of his obligation, with all his/her properties²³⁵. The creditor has the right to confiscate the properties of the debtor through compulsory execution to be performed by the execution organs in case the obligations arising of this is not fulfilled²³⁶. This way, the creditor is protected by the rule of law. The liability in this sense is called “*liability with...*”²³⁷.

Another definition of the liability is the obligation of compensation of the damage suffered as a result of the contrary actions of an individual to the general codes of conduct or any obligation undertaken²³⁸. In this type of liability, “*why*” the debtor is held liable is examined. Although the first thing that comes to mind is the tort liability, civil liability does not occur only with tort liability in private law. Breach of contractual obligations also constitutes unlawfulness. Accordingly, there shall be tort liability in case of breach of general codes of conduct and there shall be liability for the actions that breach obligations in case of breach of contractual obligations²³⁹. This type of liability is called “*liability from...*”.

²³⁴ Selahattin Sulhi Tekinay, Sermet Akman, Haluk Burcuoğlu and Atilla Altop, *Borçlar Hukuku*, Reviewed and Expanded 6. Edition (İstanbul, 1989), p. 20; Eren, p. 83; Oğuzman and Öz, Vol. I, p. 16. Today the liability of the debtor for his/her actions that breach the obligations is only the liability of property. Holding an individual liable for his/her personality rights and limitation of his/her freedom due to the breach of obligation cannot be accepted. Cansel and Özel, p. 84; Kılıçoğlu, *Genel Hükümler*, p. 46. This is guaranteed in art. 38/8 of the Constitution, which is as “*No one shall be deprived of his/her liberty merely on the ground of inability to fulfill a contractual obligation*”.

²³⁵ Oğuzman and Öz, Vol. I, p. 16; Eren, p. 86.

²³⁶ In rare cases, the rule of law authorizes the creditor to confiscate with his/her own power, the properties of the debtor (self enforcement of a right) art. 64/3 of TCO and art. 981 of TCC can be given as an example to these exceptions. Eren, p. 83.

²³⁷ Eren, p. 85-86; Oğuzman and Öz, Vol. I, p. 16.

²³⁸ Oğuzman and Öz, Vol. I, p. 17. “*liability from...*” is used in three different meanings in the doctrine. The first one is a broad liability and it covers both the non-contractual liability and the liability for breach of contractual obligation. The second one is a narrow liability and it accepts only non-contractual liability. The last one is the narrowest liability. Within this context, the cases of strict liability regulated by special laws are expressed (absolute and risk liability). Eren, p. 511; Gökhan Antalya, *Borçlar Hukuku Genel Hükümler*, Vol. II, 2. Edition (İstanbul: Legal Kitabevi, 2018), p. 1. In this study, we shall interpret the term of liability as the broadest liability in order to describe the subject more extensively and plainly.

²³⁹ Haluk Tandoğan, *Türk Mes'uliyet Hukuku*, Exact Copy of 1961 First Edition (İstanbul: Vedat Kitapçılık, 2010), p. 5; Oğuzman and Öz, Vol. I, p. 17; Antalya, Vol. II, p. 1.

According to “*liability from...*”, the debtor (*damaging party*), is required to compensate the damage incurred by the creditors (*injured party*)²⁴⁰. The common point of the illegal actions such as the breach of the general codes of conduct or breach of obligations is that they result in compensation obligation. Due to this it can be said that liability constitutes the basis of compensation obligation. This type of liability can also be called “*compensation law*” based on the reasons mentioned²⁴¹. In this study, the liability of the data control within this frame shall be discussed and the compensation of the damages caused by the data controller shall be examined within the scope of “*liability from...*”.

1.1.Reasons of the Liability

The injured party is directly affected from the damaging activities of both himself/herself and a third party on his/her properties and personality²⁴². For example, in case of any damage to arise as a result of an individual’s running into a wall by his/her car, such individual is required to bear the results of such damage. However, the reason of this accident may be the individual’s own fault or the fault of the service station repairing the individual’s car, which delivered the car with failing brakes without paying the due attention and care. In this case, the rule of law considers that this principle would cause certain injustice and lays the burden of remedy for the damage suffered, on the third parties in the presence of some grounds²⁴³.

The reasons which justify laying the burden of the compensation of the damage suffered, on the third parties is called “*reasons of the liability*”²⁴⁴. These reasons are three as fault, contract and law. In case of presence of these reasons, an individual shall be able to demand the compensation of the damage from a third party.

²⁴⁰ Şaban Kayıhan and Mustafa Ünlütepe, *Borçlar Hukuku Genel Hükümler*, 6. Edition (Ankara: Seçkin Yayıncılık, 2018), p. 38; Tandoğan, p. 3; Tekinay, Akman, Burcuoğlu and Altop, p. 18.

²⁴¹ Eren, p. 510; Antalya, Vol. II, p. 1; The term “Liability Law” is used in order to express all the cases related to the liability arising of the breach of contract and tort liability. Tekinay, Akman, Burcuoğlu and Altop, p. 641.

²⁴² Antalya, Vol. II, p. 9; The proverbs such as “Injured one bites the bullet”, “An ember burns where it falls”, “What can’t be cured must be endured” express this opinion. Eren, p. 511.

²⁴³ Tandoğan, p. 8; Eren, p. 512; Hüseyin Hatemi and Emre Gökyayla, *Borçlar Hukuku Genel Bölüm*, 4.Edition (İstanbul: Vedat Kitapçılık, 2017), p. 113.

²⁴⁴ Eren, p. 512.

1.1.1. Fault

The main reason for a person to be liable for a damage suffered is fault. A person damaging the others with his faulty behaviors and unlawful actions which are not approved by the rule of law is required to compensate this damage²⁴⁵. Art. 49 of TCO clearly regulates this. According to this article, “*Any person who, by his faulty and unlawful behavior, causes damage to another is obliged to provide compensation*”. The fault is required both in the tort liability and contract liability.

1.1.2. Contract

Another reason of liability is contract. Under a contract, a person, without any fault on his/her side, may undertake the compensation of any damage that a third party may incur. In this case, the debtor of the contract undertakes the remedy of the damages, in other words, liability for the damage the creditor incurred or shall incur. Accordingly, the fault of the debtor shall not be sought. A person guaranteeing the debt of a debtor pays the debt in case such debt is not paid or obligation of the insurer to compensate the damage if the risk is realized in insurance contracts in consideration of premiums can be given as examples to this state²⁴⁶.

1.1.3. Provision of Law

Sometimes a law or a provision of the law constitutes the reason of the liability. In this case, fault or contract is not required in order to have a third party compensate the damage to the injured party. The law directly imposes the third party, the compensation of the damages to be incurred by such persons. This reason of liability specifically arises in strict liability and compulsory insurance cases, especially the risk liability²⁴⁷.

²⁴⁵ Tandoğan, p. 8; According to the principle of fault, in order for a third party to compensate the damage, such damage is required to be result a faulty behavior of such third party. Otherwise, the injured party bears the consequences himself/herself. Antalya, Vol. II, p. 9.

²⁴⁶ Eren, p. 512.

²⁴⁷ In the liability law, there is a tendency since the 19th century for transferring the responsibility to the insurance institutions due to the increase of social thought and danger risks. This state also accelerated the development of strict liability. In activities which accommodate “special and typical danger”, the law maker makes regulations that mandate the compulsory and general insurances. This way, the compensation of the damage suffered is provided by these institutions. Antalya, Vol. II, p. 5; Eren, p. 513.

1.2.Liability for Personal Data Protection

1.2.1. Provisions related to Civil Liability in EU Legislation

The issue of liability is regulated in art. 23²⁴⁸ of the Directive no 95/46/EC, which is one of the most important regulations in EU concerning the personal data protection legislation, and which LPPD is based on. According to this provision, the data controller is responsible for all the damages suffered as a result of any data processing activity which is contrary to the personal data protection law²⁴⁹. Accordingly, emphasis is made on the liability of the data controller for the damages to be suffered as a result of data processing activities which are contrary to the Directive and the national laws of the member states. According to the Directive, the data controller is solely responsible for unlawful processing. There are no provisions concerning the liability of the data processor. However, it is stated in the art. 16 of the Directive, that the data processor cannot process the personal data, unless with the instruction of the data controller.

In GDPR, the sharing of the responsibility between the data controller and the data processor is described in more detail. Under the title “*Right to Compensation and Liability*” of the art. 82²⁵⁰ of GDPR, it is stated that the data controllers or the data processors shall be responsible for the material and moral damages suffered in case of

²⁴⁸ “(1) Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.(2) The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.”

²⁴⁹ Alsenoy, p. 273.

²⁵⁰ According to the art. 28 of the Data Protection Regulation of the European Union “ (1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. (2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. (3) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. (4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. (5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.”

infringement of the Regulation. This way, the scope of the persons to be responsible for the infringements to occur due to the personal data processed is enlarged. Although not a data controller within the frame of GDPR, the persons processing such data as data processors under any authority granted shall also be responsible for the infringements to occur²⁵¹. Together with this regulation, the data processor shall also directly be responsible to the data subject when unlawful actions are taken²⁵².

Art. 82 of GDPR not only expanded the scope of the liability, but it also regulated in detail, the conditions and scope for which the data controller and the data processor shall be held liable. Accordingly, the data controllers shall be held liable for the damages caused by any and all activities violating the Regulation regardless of their fault rate. The liability of the data processors is interpreted in a narrower sense. In art. 82/2 of GDPR, it is stated that the data processor shall be liable for the damage caused by processing only where he/she has not complied with obligations of this Regulation specifically directed to the data processors or where he/she has acted outside or contrary to lawful instructions of the data controller. Accordingly, the borders of the liability of the data processor are drawn.

According to the art. 23/2 of the Directive no 95/46EC, the data controller may be exempted from this liability, in whole or in part, if he/she proves that he/she is not responsible for the event giving rise to the damage. As it could be understood from this provision, the fault of the data controller is not sought for the data controller's liability with respect to the damage to arise as a result of the unlawful processing of the personal data. In other words, in compliance with the Directive no 95/46EC, the data controller cannot be relieved from the liability if he/she proves that he/she is not faulty²⁵³. There is no change in GDPR concerning this, and in art. 82/3, it is stated that a data controller and data processor shall be exempt from liability if he/she proves that he/she is not in any way responsible for the event giving rise to the damage. Accordingly, GDPR made an regulation parallel to the Directive no 95/46/EC and held the data controller liable in compliance with the provisions of strict liability. The

²⁵¹ This is because, in the Directive 95/46/EC, it was regulated that the injured data subject could only demand compensation from the data controllers. Ayşe Nur Akıncı, p. 34; Alsenoy, p. 284.

²⁵² Alsenoy, p. 282.

²⁵³ Alsenoy, p. 273.

conditions required for the data controller to be relieved of liability shall be examined separately in the fault section.

In the 4th and 5th paragraphs of the art. 82 of GDPR, the joint liability of the data controller and the data processors is addressed. Accordingly, in cases where the civil liability of the data processor and data controller arises, the data subject can demand the whole damage from both of them. The party paying the whole damage to the data subject from shall be entitled to claim back from the other party that part of the compensation corresponding to their part of responsibility for the damage.

As it could be understood from the regulations mentioned above, both in the Directive and the Regulation it is expressed that the data controller shall compensate the damage suffered in case of unlawful processing of the personal data. In this study, these provisions shall be examined in more detail, when appropriate.

1.2.2. The Current State in Turkey

In our country, there is no special provision related to the civil liability of the data controller in the LPPD no 6698 in force concerning the personal data protection. Instead, the general provisions are referred to. Protection Authority, which is the administrative remedy, with respect to the unlawful processing of the personal data within the frame of LPPD, or has the right to file a case in compliance with the compensation provisions arising of the general liability law. This right of the data subject is regulated in art. 11/1(ğ) of the LPPD. According to this provision, the data subject has the right “*to request compensation for the damage arising from the unlawful processing of his personal data*”. The data subjects may file a case before the judicial or administrative jurisdiction based on the legal status of the data controller²⁵⁴.

Before the LPPD took effect, in cases where the personal data processed unlawfully damages the personal rights of an individual, the compensation was provided within the frame of the provisions of the civil code protecting the personality²⁵⁵. However, a need to have a separate regulation for personal data have arisen as a result of the

²⁵⁴ See: LPPD Preamble, p. 13.

²⁵⁵ For detailed information concerning the protection of personal data within the scope of the personal rights before the LPPD took effect, see: Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması* (Ankara: Çakmak Yayınları, 2010).

increase of damage risk to occur based on the spreading of personal data processing activities and unlawful personal data processing²⁵⁶. As the LPPD took effect, both the borders of the unlawfulness factor were drawn clearly²⁵⁷ and the awareness in the society concerning the personal data protection was raised²⁵⁸.

The provisions regulated by the LPPD bring a protection which is not provided by the provisions of TCC concerning the protection of the general personality rights and in a sense, these complete the general provisions²⁵⁹. Because, the protection of personal data, which are considered within the scope of the protection of private life in the general provisions, may not be sufficient in order to protect the individuals only within the frame of the private life. It is possible to collect and analyze the personal data not related to the private life of a person, which look simpler and less harmful and to draw the profiles of the individuals. LPPD enables such data to be included within the scope of protection.

Although there are provisions protecting the personality in the provisions of the TCC, another benefit of a special law like LPPD for the protection of personal data is that LPPD takes preventive measures before the violation of the personal rights of the individuals. The regulations such as the basic principles concerning the data processing activities, obligation of the data controller to inform the data subject, obligation of the registry of the data controllers and the requirement of taking the measures and precautions in order to protect the personal data are mainly preventive

²⁵⁶ Only in January 2019, 1,769,185,063 records were leaked to the third parties illegally as a result of data violations and cyber attacks. <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-2019-1769185063-records-leaked> (Access Date: 15.03.2019).

²⁵⁷ The general principles for personal data processing are determined in the art. 4, legality conditions are specifically examined in the art. 5 and 6, the obligations of the data controller and the rights of the data subject are regulated in the art.10, 11 and 12 of LPPD. Accordingly, the ambiguities in determining the illegalities in the processing or protection of the personal data are eliminated.

²⁵⁸ One of the main purposes of the Personal Data Protection Authority, which is established by LPPD, is to raise awareness in the society for the protection of the personal data. For this purpose, many activities are carried out by the Authority. For the activities carried out by the Authority in order to raise awareness in the society, see: <https://www.kvkk.gov.tr/Icerik/2020/Etkinlikler>.

²⁵⁹ Küzeci, p. 383.

provisions²⁶⁰. However, the provisions in TCC and TCO protecting the personality are mainly functional following the occurrence of an assault directed to the personality²⁶¹.

The data controller or the data processors sometimes process data as based on a contract and sometimes process the data within the frame of the lawfulness conditions required by the law without any contract. However, sometimes the data controllers are not attentive to the protection of the personal data when processing the data based on a contract concluded with the data subject and cause material and moral damage to the person and sometimes give rise to damage as a result of unlawful processing of the data, without any contract²⁶². Or, the personal data processed lawfully may be acquired by the third parties due to the data controllers' lack of attention and care and this way, the data subjects may suffer material and moral damage.

If the data controller acts contrary to the general codes of conduct without any contract and as a result he/she is under the obligation of compensating the damages to arise due to the unlawful personal data processing, then this shall result in tort liability. As also emphasized in the LPPD, the person whose personal rights²⁶³ are violated as a result of unlawful processing of his/her personal data shall apply to the general provisions for the compensation of the damages. Accordingly, the data subject may apply to the provisions of the art. 23, 24 and 25 of the TCC or the art. 49 and 58 of the TCO. While the art. 23 of TCC protects the personal right against violation through legal transactions, art. 24 of TCC protects the personal right against the unlawful assaults to

²⁶⁰ Küzeci, p. 383.

²⁶¹ In art. 25 of TCC, when the cases for protection of the personality are examined, taking an action for prevention of assault, determination of the assault, the right to demand compensation for physical and moral damages are the regulations to be performed following the assault. Although the case for prevention of the assault is regulated, this is applied at a narrower scale in practice. Other than these, the provisions of the art. 49 and 58 of TCO are the provisions with respect to the compensation of the damage following the assault. According to *Antalya*, the prevention of the damage is the secondary purpose in the compensation liability. This is because if the damaging party knows that the compensation liability is to arise, then this shall drive such person to act more carefully and attentively. *Antalya*, Vol. II, p. 4.

²⁶² There are no limitations on the amounts and types of the damage to be claimed by the data subject. The data subject may demand the compensation of both the material (for example loss of revenue) and moral (for example loss of reputation, loss of trust, psychological damage) damages arising of the data processing activities. *Alsenoy*, p. 277.

²⁶³ While the protection of the personal data was examined within the scope of protection of private life in the first periods, it was removed from the fundamental right of the protection of private life together with the German Constitutional Court's "*Census Decision*" in the future periods and it became a separate right within the scope of the right for protection of personal data. The right for the protection of personal data constitutes a distinct outlook of the protection of personality in terms of private law. *Küzeci*, p. 379.

be come from outside. If it is determined that the personal data is processed unlawfully, then art. 25 of TCC and art. 49 and 58 of TCO can be referred to in order to demand compensation in compliance with the provisions of private law. We touch upon only mentioning these here since our explanations concerning these articles shall be made in the following sections.

In some cases, the data controller performs the processing activities under a contract concluded with the data subject and liability for breach of obligations arises during this data processing. Although each state contrary to the contract during the processing of the personal data also constitutes contrariety to the general codes of conduct and results in tort liability, the provisions of liability due to the breach of obligations shall result in favor of the damaged party and this type of liability shall be examined specifically within the frame of this study.

Finally, if the data processing activities are realized although a contract is not established yet between the data controller and the data subject, the data controller shall be liable for the damage to arise of this relation, within the scope of culpa in contrahendo liability, which became more of an issue in the recent periods²⁶⁴.

For the compensation obligation to arise, there should be a casual relation between the damage and the unlawful action²⁶⁵. In Turkish law, the requirement of fault in unlawful processing of the personal data is controversial²⁶⁶. The dominant opinion in this area is that the fault liability is the basis, since the strict liability of the data controller is not specifically regulated in LPPD and a reference is made to the general provisions²⁶⁷.

We shall examine in this study how the data controller shall be responsible for the damages to arise as a result of the data controller's data processing activity within the

²⁶⁴ In this type of liability, there is the state of damaging the other party due to the actions that are contrary to the quasi-contract trust relationship based on the fairness principle between them during the negotiations of the contract prior to the establishment of such contract. Although Culpa in Contrahendo liability is controversial type of liability in the doctrine, it is considered as a separate source of liability other than the liability arising of tort and breach of obligation. Ümit Gezder, *Türk- İsviçre Hukukunda Culpa in Contrahendo Sorumluluğu* (Ankara: Beta Yayınları, 2010), p. 13; Kayıhan and Ünlütepe, p. 55; Kılıçoğlu, p. 89.

²⁶⁵ Antalya, Vol. II, p. 205; Abdulkemim Yıldırım, *Türk Borçlar Hukuku Genel Hükümler*, 7.Edition (Ankara: Monopol Yayınları, 2018), p. 176; Hatemi and Gökyayla, p. 135.

²⁶⁶ Başalp, *Kişisel Verilerin Korunması*, p. 65. The fault of the data controller is not sought in cases where there is service fault, employer's liability or risk liability.

²⁶⁷ Gürpınar, p. 690.

scope of “*liability from...*”. Accordingly, we shall try to find the answers to the questions of, in which cases, how and by whom, the damages to arise as a result of unlawful processing of the personal data shall be compensated.

2. THE LIABILITY OF THE DATA CONTROLLER ARISING OF THE TORT RELATION

In the modern society in which the personal data is considered as power, the states, companies or some private persons tend to collect and analyze the personal data of the individuals. This way, they shall have more information about the individuals and shall have the capability to direct them easily. The personal data of the individuals may be processed due to this and the reasons mentioned above. In this case, if there is no lawful ground in the processing of the personal data, then the personal rights of the individual shall directly be interfered and this shall give rise to tort liability.

The data subject whose personal rights are violated as a result of the unlawful processing of the personal data can apply to the provisions in art. 25 of TCC protecting the personality and the provisions in art. 49 and 58 of TCO and have such damage compensated. According to art. 49 of TCO “*Any person who, by his faulty and unlawful behavior, causes damage to another is obliged to provide compensation.*” As it can be understood from this provision, the tort liability constitutes the basis of compensation obligation²⁶⁸. The difference of tort liability from the contractual liability is that it occurs in cases where actions contrary to the general codes of conduct are performed, rather than a breach of an obligation previously undertaken²⁶⁹.

As a rule, tort liability is based on the fault of the party performing the damaging activity according to TCO. In all cases not regulated by a special liability provision, the fault of the offender is required for the occurrence of tort liability²⁷⁰. In other

²⁶⁸ Mehmet Refik Korkusuz and Mustafa Halit Korkusuz, *Hukuk Başlangıcı*, 4.Edition (İstanbul: Beta Yayınları, 2018), p. 64; Oğuzman and Öz, Vol. I, p. 1; Yıldırım, p. 165.

²⁶⁹ Tekinay, Akman, Burcuoğlu and Altop, p. 641; Antalya, Vol. II, p. 17; Oğuzman and Öz, Vol. I, p. 1.

²⁷⁰ Tandoğan, p. 11; M. Kemal Oğuzman and Turgut Öz, *Borçlar Hukuku Genel Hükümler*. V. II. 16.Edition (İstanbul: Vedat Kitapçılık, 2018), p. 11.

words, the rule in tort liability is the liability that is based on the fault and the exception is the strict liability cases²⁷¹.

For the occurrence of tort liability, first it is required that the data controller performs an unlawful action. Material or moral damage should arise as a result of such action and there should be a legally acceptable relation, connection between this damage and the action. Finally, the data controller is required to be faulty as a rule²⁷². However, although this is the rule, strict liability may arise in some cases.

2.1.Unlawful Action of the Data Controller

2.1.1. Unlawful Action

One of the fundamental conditions for the emergence of tort liability is the existence of an unlawful action. If the person from whom compensation shall be demanded does not have any actions, then it shall not be possible to talk about liability²⁷³. Action is the willful behavior of an individual presented as performance or non-performance²⁷⁴. Within the context of protection of personal data, the actions which the data controller shall perform in the form of performance are the data processing activities. Data processing concept is an upper concept and what is desired to be described by this is “*any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof*”.

For any action to occur in the form of non-performance, such performer is required to have the obligation of performing such action²⁷⁵. Article 12 of the LPPD imposed on

²⁷¹ Şahin Akıncı, *Borçlar Hukuku Bilgisi Genel Hükümler*, 10. Edition (Konya: Sayram Yayınları, 2017), p. 151; Korkusuz and Korkusuz, p. 64.

²⁷² Some authors categorize the conditions of the tort liability into five parts as action, damage, appropriate casual relation, fault and unlawfulness. Şahin Akıncı, p. 136; Yıldırım, p. 165; In this study we are examining it under four titles because we combined the factors of action and unlawfulness. For the authors examining the tort liability conditions under four groups, see: Antalya, Vol. II, p. 39; Hatemi and Gökyayla, p. 116; *Kaneti* on the other hand, examined the tort liability factors as action, unlawfulness, fault and damage. He examines the casual relation as a subtitle of the action. Selim Kaneti, *Haksız Fiilde Hukuka Aykırılık Unsuru*, (İstanbul: Kazancı Hukuk Yayınları, 2007), p. 15 ff.

²⁷³ Oğuzman and Öz, Vol. II, p. 13; Antalya, Vol. II, p. 17; There are also exceptions to this state. Specifically in strict liability cases, there are cases in which the person held responsible is held responsible without any action of such person. The most apparent example to this is the liability of the owner of the building or property.

²⁷⁴ Antalya, Vol. II, p. 17; Tandoğan, p. 13; Oğuzman and Öz, Vol. II, p. 13. According to another definition, action is defined as the product of the willful behavior of an individual. Kaneti, p. 15.

²⁷⁵ Yıldırım, p. 166; Oğuzman and Öz, Vol. II, p. 13; Tandoğan, p. 18; Antalya, Vol. II, p. 64.

the data controller to take all the technical and administrative measures required for providing the appropriate security level in order to prevent unlawful processing and access of the personal data which are processed lawfully and to enable the protection. Accordingly, any action which the data controller shall realize in the form of non-performance is the state of not taking the security measures which are required in order to protect the personal data processed.

Another behavior to occur in the form of non-performance, which constitutes unlawfulness, is non-notification of the data subject and the Authority by the data controller in compliance with art. 12/5 of the LPPD, in case the processed personal data are unlawfully acquired by another person. The unlawful action factor shall occur in case the data subject does not inform²⁷⁶. The data subject shall be responsible for the compensation of the damage to be suffered as a result of realization of the other conditions. In case the processing reasons of the lawfully processed personal data are no more valid, the civil liability of the data controller shall arise if these are not deleted, destroyed or anonymized by the data controller.

According to art. 24 of TCC, when there is an unlawful assault²⁷⁷ to the personal rights of a person, then such person may claim protection from the judge against the individuals who made the assault. An attack to the personal rights means an attack made to all the factors included within the scope of the personality of a person²⁷⁸. With this provision, the personal rights are protected in general. This is because it is not possible to count one by one the factors that make up a personality. Since the personal data constitute an special outlook of the personal values, they are protected within the scope of this provision.

²⁷⁶ On January 19, 2019, social video sharing website DailyMotion informed that the accounts of the users were unlawfully accessed by sending a mail both to the users who are influenced by the data violation and to French Data Protection Authority CNIL in compliance with the GDPR. Otherwise, it would have acted contrary to the art. 33 and 34 of the GDPR and its liability shall increase due to the damages to be suffered and shall be subject to administrative fine. For the mentioned event, see: <https://www.zdnet.com/article/dailymotion-discloses-credential-stuffing-attack/> (Access Date: 15.02.2019).

²⁷⁷ The issue of unlawfulness is an issue that is independent of fault and if required, the claimant is expected to prove. Tekinay, Akman, Burcuoğlu and Altop, s. 643.

²⁷⁸ Oğuzman, Seliçi and Özdemir, p. 218.

In case the data controller or the data processor performs processing activities which are contrary to the provisions provided by the LPPD, then such processing activity is unlawful²⁷⁹. In case the other tort liability conditions exist, then the data controller's tort liability shall occur.

For example, if a photographer takes the photos of his customers and keeps these on his own system and displays these on the shop's showcase without obtaining the consent of the customers, this state constitutes a direct violation of the personal rights. Or the data concerning the victim of an outdated event are disclosed again without taking the consent of the data subject, then this shall constitute an attack to the personal rights²⁸⁰. This state constitutes an abuse of the honor and dignity, which are personal right values, violation of the privacy and directly breach of the personal data protection rights.

Another example that can be given to this is the duplication and use of a public photograph, shared on a social sharing platform, for commercial purposes, which shall constitute a violation with respect to the protection of personal data²⁸¹. This is because the purpose of the data subject making such personal data public is to use it in his/her own account and for communication with those that are close to him/her. Sharing these photographs for commercial purposes without the consent of the data subject shall violate the individual's personal data protection right.

Unlawful processing of the personal data is considered as a violation of personal rights²⁸². However, there are lawful grounds in the LPPD concerning the processing of personal data. Since lawful grounds are regulated in LPPD, which is a more specific

²⁷⁹ If an action violates a personal right or absolute property right, then this is unlawful unless there is a reason of lawfulness. Hatemi and Gökyayla, p. 116; Hatemi, *Kişiler*, p. 68; Supreme Court, 4.CC., D.27.06.2016, M. 2015/7330, D. 2016/8358- Legalbank Elektronik Hukuk Bankası, (Access Date: 10.01.2019).

²⁸⁰ Supreme Court ACC., D. 17.06.2015, M. 2014/56, D. 2015/1679 – Legalbank Elektronik Hukuk Bankası, (Access Date: 10.01.2019).

²⁸¹ This state is considered within the scope of the violation of personal rights in one of the decisions of the Supreme Court. According to this decision, consent given for the publication of a photograph on a website for cultural and introduction purposes does not mean the duplication and use of such photograph by others without consent for commercial purposes. For the relevant decision, see: Supreme Court 11. CC., D. 21.06.2010, M. 2009/1555, d. 2010/7121- Legalbank Elektronik Hukuk Bankası, (Access Date: 11.01.2009).

²⁸² Mine Kaya, *Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması* (Ankara: Seçkin Yayınları, 2015), p. 101; Özdemir, p. 107; Gürsel, p. 53, Ayözger, p. 233.

law when compared to the Civil Code and Code of Obligations, the provisions of the LPPD are taken into consideration with respect to the compensation obligation of the data controller²⁸³.

2.1.2. The Lawful Grounds on the Processing of Personal Data

For the occurrence of tort liability due to the data controller's processing of personal data, it is required that such processing is unlawful. Article 20/3 of the Constitution states that the personal data "*can be processed only in cases envisaged by law or by the person's explicit consent*" and the protection of personal data is considered within the scope of the fundamental rights and freedoms.

As it can be understood from this provision, processing of personal data is unlawful as a rule. Limitation of this right, in other words, lawful processing of the personal data is possible only if provided by law or by the explicit consent of the data subject²⁸⁴. Likewise, art. 13 of the Constitution regulates that the fundamental rights and freedoms can only be limited by the laws²⁸⁵.

The lawful grounds for the processing of personal data are listed in the art. 5 and 6 of LPPD. Accordingly, the borders of when the personal data could be processed lawfully were drawn. However, it should be underlined here that, the data controller is required to act in compliance with the general principles regulated in the 4th article even in the presence of these conditions. Otherwise, the processing activity shall be unlawful.

According to the general provisions, an activity cannot be considered as unlawful, as long as such activity itself is not contrary to any obligation of conduct. Due to this

²⁸³ The reasons of general lawfulness for the tort liability are listed in art. 63 of TCO. These are as "*behavior that it is mandated by law and stays within the limits of such law, the injured person's consent, a superior private or public interest exists, the necessary defense, the legitimate self-defense or the compulsory states*". This provision which is regulated as a general provision is narrowed more in case of violation of the personal right. According to art. 24/2 of TCC, the tort liability of the damaging party shall arise for the personal right violations except "*the consent of the person whose personal right is damaged, superior private or public interest and use of authorization conferred upon by the laws*".

²⁸⁴ In case of contrariety to the general codes of conduct in private legal liability, in order to claim the existence of the lawfulness reasons it is required that it is specified conclusively by a legal regulation. Lawfulness reasons should not be imposed by filling the legal gaps. Hatemi and Gökyayla, p. 123.

²⁸⁵ For detailed information about the fundamental rights and freedoms being only restricted by the law, see: Ergun Özbudun, *Türk Anayasa Hukuku*, 15.Edition (Ankara: Yetkin Yayınları, 2014), p. 111-123; Hasan Tahsin Fendoğlu, "2001 Anayasa Değişikliği Bağlamında Temel Hak ve Özgürlüklerin Sınırlanması (13th Article of the Constitution)", *Elektronik Sosyal Bilimler Dergisi*, Vol.1, 2014, <http://dergipark.ulakbim.gov.tr/esosder/article/view/5000067866> (Access Date: 16.02.2019)

reason, the burden of proof for unlawfulness belongs to the injured party²⁸⁶. However, the attacks to the personal values are accepted to be unlawful, as a rule²⁸⁷. Accordingly, the offender claiming that the action performed is lawful is required to prove this. According to this, unlawfulness is the rule in processing the personal data and the presence of lawful grounds is the exception. This is because a person claiming that processing is performed as based on the lawful grounds in the LPPD is required to prove this²⁸⁸. Accordingly, the data controller can only be relieved from the liability against the data subject claiming that the personal data are unlawfully processed, by proving the lawful grounds. Otherwise, the personal data processing performed shall be considered as unlawful.

It is clearly regulated in the art. 5/2 of GDPR, within the principle of accountability, that the burden of proof for the lawfulness of the personal data processing activity belongs to the data controller. According to this provision, the data controller is required to prove that he/she acts in compliance with the data protection principles²⁸⁹. This state is specifically expressed in the other provisions of the Regulation. For example, in the art. 7 of the Regulation, the burden of proof for evidencing that the data subject consented the processing activity is given to the data controller. Moreover, according to the art. 24 of GDPR, the obligation of taking the appropriate technical and organizational measures in order to provide and prove the processing activity's compliance with the Regulation is an example to this state²⁹⁰.

2.1.2.1. Explicit Consent of the Data Subject

The requirement of “*explicit consent*” which is one of the lawful grounds is regulated by both art. 5/1 and art. 6/2 of the LPPD²⁹¹. According to these provisions, the personal

²⁸⁶ Serozan, *Kişiler Hukuku*, p. 468; Tandoğan, p. 44; Hatemi and Gökyayla, p. 123.

²⁸⁷ The expression “Each assault against personal rights is considered contrary to the laws” in the art. 24/II of the TCC clearly regulates this state. For detailed information, see: Hatemi, p. 73.

²⁸⁸ With respect to laying the burden of proof for the presence of one of the lawfulness reasons regulated by art. 24/2 of TCC, on the person claiming such lawfulness see: Oğuzman, Seliçi and Oktay-Özdemir, p. 219; Hatemi, p. 72; Antalya, *Manevi Zararın Belirlenmesi*, p. 54; According to Serozan an action cannot be considered as unlawful as long as such action itself is not contrary to any behavior obligation. Due to this reason, the burden of proof for the unlawfulness is on the injured party. Serozan, *Kişiler Hukuku*, p. 468; Tandoğan, p. 44; Hatemi and Gökyayla, p. 123.

²⁸⁹ For detailed information concerning the accountability principle, see.: I. Section, 3.6. Accountability

²⁹⁰ Alsenoy, p. 282.

²⁹¹ The provisions in the law concerning the explicit consent are not only in these articles. Also the explicit consent of the data subject is required in art. 8/1 and art. 9/1 in order to transfer the personal

data processing activity cannot be performed without the explicit consent of the person. However, if the other lawful grounds in the law exist, then explicit consent is not required. Based on this, the order of examining the lawful grounds, which is frequently encountered in practice, is important. In the law generally it is emphasized as the first provision that the data cannot be processed without the explicit consent of the data subject and the other lawful grounds are listed. However, this does not mean that the explicit consent of the data subject shall be taken into account and if such consent does not exist, other lawful grounds shall be examined. On the contrary, if the other lawful grounds are present, the data should be processed first as based on these, and if such grounds are not present, then the explicit consent of the data subject should be taken²⁹². Otherwise, the explicit consent of the data subject shall be required even if the lawful grounds stated in the law exist, and this shall result in the loss of labor and time and also shall cause the data subject to be mistaken in his/her intention.

2.1.2.1.1. The Concept of Explicit Consent

Explicit consent is defined as “*freely given, specific and informed consent*” in art. 3/1(a) of the LPPD²⁹³. As it could be understood from this definition, the concept of explicit consent is based on three fundamental elements. Accordingly, the consent given by the data subject should be related to a specific issue, the data subject should sufficiently be informed about the processing activity and finally, should not be under any influence when notifying his/her will concerning the processing²⁹⁴. When the

data to a third party or abroad. Since processing of the personal data also covers the transfer of the data, the regulations in art. 5 and art. 6 also cover the transfer of the personal data.

²⁹² Personal Data Protection Authority, *Kişisel Verilerin İşlenme Şartları*, Ankara, 2017, p. 3. see: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf> (Access Date: 22.01.2019).

²⁹³ In the doctrine some authors stated that this definition is not a definition of explicit consent, but it is the definition of consent only. In the Regulation and the Directive no 95/46EC the term “*unambiguously*” is used in the definition of explicit consent. However, this term does not exist in the definition of the explicit consent in the LPPD. Cihan Avcı Braun, “*Kişisel Verilerin İşlenmesinde Rıza*”, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Vol. XV, Issue. 1, (2018), p. 19; GDPR art. 4/11: “*'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*”

²⁹⁴ Macenaite and Kosta, p. 156. *Article 20 Working Party* examined the explicit consent concept in four sections as the indication of the data subject’s wish, freewill, based on being informed and being related to a specific issue. *Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent*, Brussels, 2011. see: <https://www.pdpjournals.com/docs/88081.pdf> (Access Date:

explicit consent concept is defined in the reasoning of the article, it is stated that the Directive 95/46 is benefitted from and that the consent given should be explicit in a manner not to cause ambiguity²⁹⁵.

The concept of consent within the scope of LPPD and the concept of consent regulated in the art. 24 of TCC are not used in the same meaning. Although there is no conflict between two concepts of consent, the consent regulated in the Civil Code is a broader concept²⁹⁶. Both consents are the lawful grounds. However, stricter requirements are imposed for the consent regulated by the LPPD to be considered lawful. The general validity conditions required for the validity of the consent in the Civil Code are also required to exist in the consent given by the data subject for processing of the personal data²⁹⁷. However providing such conditions does not make the processing of the personal data lawful. In addition, the factors for protection of the personal data are also required to be completed.

2.1.2.1.2. Assessment of the Explicit Consent Elements

An explicit consent is required to be only for a specific issue and only limited by such issue²⁹⁸. Therefore, the data controller should inform about each data category to be processed and should demand explicit consent separately for each one. Otherwise, the consents such as “*I consent the processing of my personal data*” in a general, abstract and unambiguous manner, in which the process and data category is not definite, are invalid²⁹⁹. Moreover, demand of a single consent by the data controller for more than one processing activity also injures the explicit consent³⁰⁰. A separate consent should

01.01.2019). In this study, we consider it appropriate to examine the data subject’s consent wish to be shown with a positive behavior, within the frame of requirement as to form.

²⁹⁵ See: LPPD Preamble, p. 7; In the Directive, explicit consent was required only for personal data of special nature, however, in our law and in GDPR, explicit consent was required both for the processing of the ordinary personal data and personal data of special nature. For detailed information see: Dülger, pp. 22-30.

²⁹⁶ Article 29 Data Protection Working Party, *The Definition of Consent*, p. 6.

²⁹⁷ In our civil code, for the validity of the consent, the will is required to be stated explicitly, the consent given should be given consciously and with freewill by anticipation of the results of refraining and finally, the consent given should not be non-ethical. Oğuzman, Seliçi and Oktay-Özdemir, p. 220.

²⁹⁸ Article 29 Data Protection Working Party, *The Definition of Consent*, p. 17; Dülger, p. 24.

²⁹⁹ Personal Data Protection Authority, *Açık Rıza*, Ankara, 2017, p. 4. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf> (Access Date: 10.07.2018); Macenaite and Kosta, p. 158.

³⁰⁰ Çekin, *Kişisel Verilerin Korunması*, p. 60.

be given by the data subject for each processing activity (*collection, storage, transfer to the third parties etc.*). Finally, if the personal data processed lawfully are to be used for a different purpose, then the consent of the data subject should be taken again³⁰¹.

The reason that the explicit consent is based on information is that a person has the right to know to what, to which extent, for which purpose and which means he/she consents during the processing of the personal data, which is considered to be a sacrifice from his/her personal rights. Providing information to the person concerning which personal data shall be processed, how long these shall be retained or with which means they shall be processed, is not sufficient, at the same time it is required to provide information about the consequences of the consent to be given by the data subject³⁰². Informing the data subject is a significant reflection of the right of self determination³⁰³. Taking the consent as based on informing is also a requirement of the principle of fairness and transparency. Accordingly, the information to be given to the data subject should be easily accessible, understandable and should be in plain language³⁰⁴.

Finally, it should be expressed that when the data subject consents for the processing of the personal data, he/she should be aware of the results of this behavior and should not be under any influence to injure his/her will. In other words, when the data subject gives consent which means the limitation of his/her personal rights, he/she should act freely and should not be under any pressure³⁰⁵. The person's freewill cannot be mentioned in case of any fraud, error, threatening to injure the person's will. Likewise, if a person does not have real or free right of choice or if consent is not given or if consent is withdrawn, then the consent given by freewill cannot be mentioned in case of occurrence of an event to injure the data subject³⁰⁶.

³⁰¹ Dülger, p. 24.

³⁰² Personal Data Protection Authority, *Açık Rıza*, p. 5.

³⁰³ Article 29 Data Protection Working Party, *The Definition of Consent*, p. 8; Personal Data Protection Authority, *Açık Rıza*, p. 5.

³⁰⁴ Dülger, p. 25. According to Recital 58 of GDPR, when taking the consent of a child, the information given to the child should be in clear and plain language that the child can easily understand.

³⁰⁵ Macenaite and Kosta, p. 157.

³⁰⁶ Berber, p. 63; Article 29 Data Protection Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies*, Brussels, 2013, p. 5; According to 42. Recital of GDPR "... Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

When the processing of personal data is the pre-condition for the delivery of a product or the performance of a service, if processing activity is not significant for such product or service, then the consent given is required not to be considered as an explicit consent³⁰⁷. For example, if a person desiring to register in a fitness center is asked for his/her fingerprints during such registration for the entrance into the fitness center and the consent given to the company's authority, who tells that the registration shall not be completed if such fingerprint is not given, shall not be accepted as an explicit consent. This is because the company operating the fitness center may produce many other alternatives for the entrances (*card system, password system etc.*)

2.1.2.1.3. The Form of Giving the Consent

There is no provision in the LPPD stating in which form the explicit consent should be. Due to this reason, as indicated in the art. 12 of TCO "*The validity of a contract is not subject to any particular form unless otherwise specified by law*". Although this article only mentions contract, any declaration of intention giving rise to a legal consequence should be understood³⁰⁸. Based on this provision, we can say that the explicit consent is not subject to any form, unless there is a contrary provisions in Turkish law. However, as can be derived from the definition of explicit consent, the person consenting is required his/her "*positive declaration of intention*"³⁰⁹. Accordingly, if the data subject remains silent, this shall not mean that he/she consents the processing of the personal data³¹⁰. A written form is not required for this positive declaration of intention. Explicit consent can be provided via electronic means, or orally, or through a call center³¹¹. At the same time, the burden of proof belongs to the

³⁰⁷ Çekin, *Kişisel Verilerin Korunması*, p. 60.

³⁰⁸ Eren, p. 282.

³⁰⁹ Macenaite and Kosta, p. 156; Article 29 Data Protection Working Party, *The Definition of Consent*, p. 11; Personal Data Protection Authority, *Açık Rıza*, p. 3; Article 29 Data Protection Working Party, *Obtaining Consent for Cookies*, p. 4.

³¹⁰ European Data Protection Supervisor, *Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, p. 18; Macenaite and Kosta, p. 156; Prior to the profiling of the users over the internet through cookies in online behavioral advertising applications, the consents of the users are required to be taken. Due to this reason, information should be provided to the users in explicit and plain language, with respect to the issues such as the method to be used by the data contractor, the time of taking, keeping or sending the cookies. Afterwards, the consent of the users should be taken with opt-in method. Berber, p. 46.

³¹¹ In 32. Recital of the GDPR, it is stated that: "*by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing*

data controller in any dispute concerning personal data is processed under explicit consent. Due to this reason, it shall be for the benefit of the data controller, to use reliable means that can be proved, when obtaining the consent³¹².

Another important issue to be mentioned concerning the obtaining of the explicit consent is that the consent should be taken before the data processing activity. This is also understood from the wording of the law. Obtaining the consent after the data processing activity shall not make such personal data processing action lawful³¹³. The consent is required to be taken in advance also in compliance with the principle of fitness for the purpose which is one of the fundamental principles in the data processing activity. Data controller obliges to inform the data subject during the data processing. This completes the explicit consent's characteristic of being based on being informed and the processing shall be lawful as a result of the requirement of giving the explicit consent based on this information or the presence of the other lawful grounds stated in the law. However, the explicit consent to be given after the processing activity, although does not remedy unlawfulness, it may mean waiver of the compensation demand³¹⁴.

2.1.2.2. The Conditions Provided by the Law Eliminating the Unlawfulness

For the lawful processing of the personal data, the explicit consent of the data subject is not required under some conditions stated in the laws. This applies both for the ordinary personal data and the personal data of special nature. For example, in compliance with art. 75 of the Labor Code³¹⁵, the employer is required to keep a personnel file for each employee³¹⁶. Due to this reason, the employer can process all

technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.". However, the consent which is one of the lawfulness reasons in art. 24/2 of TCC can be given by an explicit declaration of intention as well as an implicit declaration of intention. Eren, p. 831.

³¹² European Data Protection Supervisor, *The Data Protection Reform Package*, p. 22.

³¹³ Çekin, *Kişisel Verilerin Korunması*, p. 58.

³¹⁴ Tandoğan, p. 32; Tekinay, Akman, Burcuoğlu and Altop, p. 661.

³¹⁵ No:4857, Adoption D.22.05.2003, O.J. No: 25134, D.10.06.2003.

³¹⁶ In art. 75/1 of the Labor Code, it is stated that "*The employer shall regulate a personnel file for each employee working in his establishment. In addition to the information about the employee's identity, the employer is obliged to keep all the documents and records which he has to regulate in accordance with this Code and other legislation and to show them to authorized persons and authorities when requested.*".

the personal data required for such personnel file without the consent of the employee.³¹⁷

In accordance with the art. 5 of the Law of Police Powers no 2559³¹⁸, taking the fingerprints of the suspects in the category of data with special nature is also considered within the frame of lawful ground³¹⁹. Moreover, in accordance with the art. 51/8 of the Electronic Communication Law, the operators can process the location data and identification data of the data subject in cases of disaster and emergencies identified in the Law no 5902³²⁰, and SOS calls³²¹.

However, processing the data with respect to the health and sexual life, which are personal data of special nature, is an exception to this. According to the art. 6 of LPPD, although the data related to health and sexual life are regulated by the law, they are only processed for the purposes of *protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing*. The data controllers to perform this processing are limited. According to the LPPD, such types of data are processed by the persons or authorized institutions or organizations under confidentiality obligation, without the explicit consent of the data subject.

2.1.2.3. Mandatory States

Art. 5/2(b) of the LPPD imposes that the personal data can be processed without obtaining any consent in the mandatory states in order to protect the life and the physical integrity of the data subject or any other third party. However, it is required that the consent of the data subject, cannot be taken due to incapability or that the consent is not deemed legally valid. The main purpose of this lawful ground is that priority is given to the right to life rather than data security if the person's life is in danger.

³¹⁷ Personal Data Protection Authority, *Kişisel Verilerin İşlenme Şartları*, p. 7.

³¹⁸ No:2559, Adoption D..04.07.1934, O.J. No: 2751, D.14.07.1934.

³¹⁹ Personal Data Protection Authority, *Kişisel Verilerin İşlenme Şartları*, p. 7.

³²⁰ For the Law on Some Arrangements Concerning the Disaster and Emergency Management Authority see: No: 5902, Adoption D. 29.05.2009, O.J. No: 27261, D. 17.06.2009.

³²¹ For detailed information about the processing of personal data in the electronic communication sector see: Ayözger, p. 160-192; Mine Kaya, p. 99-101.

When an unconscious person is taken to a hospital, processing of the personal data of such person can be given as an example to the bodily incapability³²². If a 10 year old child or a mental patient gives consent for processing his/her personal data, then there shall be legal incapability since the order of law shall not give rise to any legal consequences for such consent. In both cases, if it is vital, then the personal data can be processed without the consent of the data subject.

What should be taken into consideration here is that, the existence of a mandatory state shall be valid not only the data subject but also any third party has a life and bodily integrity threat³²³. For example, in a case where the freedom of a person is restricted, the location data or telephone tapping of some people in order to save that person's life can be considered within this frame³²⁴.

2.1.2.4. Necessity for the Conclusion or Fulfillment of a Contract

As it could be understood from the explicit wording of the Law, ordinary personal data can be processed without obtaining the consent of the parties if required, on condition that it is necessary for the conclusion or fulfillment of a contract between the parties. Accordingly, first, there should be a contractual relation between the parties for the satisfaction of the lawfulness requirement of the personal data³²⁵. It is not possible to apply this provision in case of other obligation relations such as tort or unjustified enrichment. Obtaining the customer's salary data, title deed registers and debts of the previous period by a bank to conclude a loan agreement with the customer can be given as an example to this³²⁶.

The personal data processed should be related to the parties of the contract. For example, If we assume that agreement is reached for processing the personal data of the third party in compliance with the personal data processing contract made by the data controller and the data processor. Although the processing of such person's personal data is required for the fulfillment of the contract, this shall not constitute a

³²² Ayözger, p. 26; Özdemir, p. 129.

³²³ Ayözger, p. 26.

³²⁴ Personal Data Protection Authority, *Kişisel Verilerin İşlenme Şartları*, p. 8.

³²⁵ Çekin, *Kişisel Verilerin Korunması*, p. 66; Personal Data Protection Authority, *Kişisel Verilerin İşlenme Şartları*, p. 9.

³²⁶ LPPD, Preamble, p. 9.

reason of lawfulness since such personal data processed do not belong to any of the parties of the contract.

Although the personal data to be processed is directly related to the conclusion and fulfillment of the contract, if the contract can be concluded by an alternative method, other than processing of the personal data activity, then such method should be preferred³²⁷. If there is any opportunity to achieve the conclusion or fulfillment of the contract without processing the personal data of any of the parties of the contract or by lesser intervention of the personal values, then such opportunity should be used. Otherwise, processing of the personal data shall be unlawful.

2.1.2.5. Performance of the Legal Obligation

The data controller is required to process the personal data in some cases in order to perform his/her legal obligation. In such cases, obtaining the consent of the data subject is not required for the ordinary personal data. For example, the employer is required to give to the employee a leave for marriage³²⁸. In this case, processing the employee's data concerning his/her marital status is a legal obligation for the employer.³²⁹ In this case, such personal data processed is lawful.

2.1.2.6. Making Available to the Public

Processing the personal data which are made available to the public by the data subject is not unlawful. For example, a person giving information about himself/herself and his/her family during a television program is assumed to give consent for such information to be learned. Or if a person shares his/her contact information for communication, in a public area, then processing of such contact information shall not be unlawful. It is considered that the legal interest such as the protection of privacy

³²⁷ Çekin, *Kişisel Verilerin Korunması*, p. 69.

³²⁸ The employee's leave for marriage is regulated as three days in the additional art. 2 of the Labor Code no 4857. "*Employee shall be allowed to take; three days leave of absence with pay in the event of employee's marriage or adoption of a child, or in the event of the death of the employee's mother, father, spouse, brother or sister, and child; and five days leave of absence with pay in the event of employee's spouse giving birth.*"

³²⁹ Personal Data Protection Authority, *Kişisel Verilerin İşlenmesi Şartları*, p. 10.

and self-determination right in the personal data protection law is eliminated when the person makes his/her data available to the public³³⁰.

However, it should be stated that, if a person's data are made available to the public, this shall not be sufficient for the lawful processing of such data. It is required that the data subject desires such data to be made available to the public.³³¹ In other words, if any information about a person is made available to the public without such person's will, then processing such data is unlawful. Another important point about this issue is that the data of the person which are made available to the public, should be used within the direction of the purpose of making such data available to the public. Any personal data processed for a purpose other than such purpose are also unlawful. For example, using the data of a person sharing his/her contact data on a website in order to sell his/her car, for marketing purposes shall be unlawful.³³²

2.1.2.7. Necessity for the Establishment, Exercise or Protection of a Right

In some cases, processing of the personal information is mandatory in order to acquire, exercise or protect a right. In such cases, the personal data of the data subject can be processed without consent. For example, if an employee files a lawsuit against an employer, then the employer has the right to retain the personal data of such employee for a certain period as an instrument of evidence. If such data are deleted when the labor relation is terminated, then the right to action or proof shall be taken away. What is important here is that if a right can be obtained, exercised or protected without using such personal data, then the existence of the reason of lawfulness shall not be mentioned.

2.1.2.8. Legitimate Interest

According to the art. 5/2(f) of the LPPD "*it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject*" and in such cases, the personal data processed without taking explicit consent shall be lawful. Three factors stand out for the lawful processing of the personal data when this provision is examined.

³³⁰ LPPD Preamble, p. 9; Kutlu and Kahraman, p. 55.

³³¹ Personal Data Protection Authority, *Kişisel Verilerin İşlenmesi Şartları*, p. 11.

³³² Personal Data Protection Authority, *Kişisel Verilerin İşlenmesi Şartları*, p. 11.

First of all, the data controller should have legitimate interest in processing of the personal data. Legitimate interest is any and all legal, economic or personal interest in favor of a person within the boundaries of the order of law. In order to assume that the data controller has a legitimate interest as a result of the processing activity, such interest should be more important, specific and up to date than restriction of the fundamental rights and freedoms of the data subject.³³³ What is important here is that the legitimate interest is the data controller's interest. Processing the data in favor of a third party shall be unlawful.

Within the frame of this provision, the second factor for the lawful processing of the personal data is that the personal data to be processed should not violate the fundamental rights and freedoms of the data subject. The concept of “*violation*” of the fundamental rights and freedoms is not used in the constitutional law literature. When examined within this frame, it is important to determine what is meant by the violation concept used in this provision. This is because each personal data processing activity shall, more or less, breach the personal rights of the data subject. Providing the balance of interest between the data subject and the data controller is important here³³⁴. When the legitimate interest is determined in the preamble of the Law, it is expressed that the balance of interest should be observed between the data subject and the data controller³³⁵. Accordingly, a comparison shall be made between the legitimate interests of the data controller and the restriction of the fundamental rights and freedoms of the data subject. As a result of this comparison, if the interests of the data subject are equal or superior, then the personal data can be processed lawfully without taking any consent³³⁶.

Finally, the personal data to be processed should be mandatory for realization, use or protection of the legitimate interest of the data controller³³⁷. If there are alternative

³³³ Personal Data Protection Authority, *Kişisel Verilerin İşlenmesi Şartları*, p. 14.

³³⁴ In the art. 6 of the GDPR, it is stated with respect to the legitimate interest of the data controller in processing the personal data that this interest should override the interests of the data subject in the fundamental rights and freedoms which should be protected within the frame of the art. 1. For the mentioned provision, see: art. m. 6/1(f) “*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*”

³³⁵ LPPD Preamble, p. 9.

³³⁶ Çekin, *Kişisel Verilerin Korunması*, p. 74.

³³⁷ Çekin, *Kişisel Verilerin Korunması*, p. 72.

methods for the realization of the legitimate interest, then such methods should be preferred. Otherwise, the processing activity to be performed shall be unlawful.

For example, a company owner processes the personal data of the employees in order to perform duty and role distribution during a reorganization process of the company. During this processing activity, the data related to the skills and labor of the employees concerning the work shall be processed and the employees shall be distributed to the relevant departments accordingly. This way, the relevant positions shall be filled by the competent and adequate personnel and the benefit of performing more productive shall be achieved. These processing activities shall be considered within the frame of the legitimate interest of the data controller and the processing shall be lawful.³³⁸

2.1.2.9. Assessment Concerning the Personal Data of Special Nature

Our Law considers the lawfulness reasons for processing the personal data separately as ordinary personal data and personal data of special nature like in the international texts. The reason for this is that the lawmaker desires to protect the processing of the personal data of special nature more strictly and tries to minimize the risks of attack to the moral areas of the individual. As a result, the personal data of special nature are subject to strict processing prohibition.

In compliance with the art. 22/1(ç) of LPPD, adequate measures should be taken by the Board in any case for processing the personal data of special nature. The data controller shall not be relieved of liability even if there is data subject's consent or in cases determined by the law, if he/she does not perform such measures determined by the Board.

The most important condition for processing the personal data of special nature is to obtain the explicit consent of the data subject. All types of personal data can be processed if the explicit consent of the data subject is taken lawfully. However, taking the explicit consent of the data subject is not enough for lawfulness. The basic principles in the art. 4 of the LPPD should also be taken into account. Another reason of lawfulness for processing the personal data of special nature is the laws. If there is an provision in the laws with respect to the processing of personal data of special

³³⁸ Personal Data Protection Authority, *Kişisel Verilerin İşlenmesi Şartları*, p. 14.

nature, then such data can also be processed. For example, according to Judicial Records Law no 5352³³⁹ the Ministry of Justice can process the criminal conviction data of the individuals which are data of special nature.

However, processing of some of the personal data of special nature is subjected to stricter conditions. These data can be called as *reinforced data of special nature*³⁴⁰. Arrangement by the law is not sufficient for the processing of such data without the explicit consent of the data subject. In art. 6/3 the LPPD, it is stated “*data relating to health and sexual life may only be processed, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing*”. Moreover, realization of these purposes is not sufficient for the lawful processing of such data, it is also required that these are processed by any person or authorized public institutions and organizations that have confidentiality obligation. Due to this reason, the health data processed by the authorities of the Ministry of Health or the Social Security Institution are considered within this frame³⁴¹.

2.2.Damage as a Result of Processing of the Personal Data

In tort liability, unlawful actions of a person give rise to compensation obligation only if such action damages others³⁴². In other words, the compensation obligation does not arise if any damage is not incurred as a result of the unlawful actions of a person³⁴³. Because the purpose in private law liability is not to punish the unlawful action, but to compensate the damages that arise as a result of such action³⁴⁴.

³³⁹ Law No: 5352, Adoption D. 25.05.2005, O.J. No: 25832, D.01.06.2005.

³⁴⁰ Such data are named as data of special nature in the law and the doctrine and no other expression was used. However, these depart from the other data of special nature since they are regulated separately by the law and stricter conditions are required for processing. Due to this reason, we are using the concept of “*reinforced data of special nature*” in our study in order to emphasize this distinction.

³⁴¹ LPPD Preamble, p. 10.

³⁴² Oğuzman and Öz, Vol. II, p. 38; Kayıhan and Ünlütepe, p. 261.

³⁴³ Hatemi and Gökyayla, p. 130.

³⁴⁴ Oğuzman and Öz, Vol. II, p. 39; However in penal law, if an unlawful action is a result of the typical actions in the law, it shall be punished whether or not there is damage. For example, when a gun is fired towards someone for killing such person, the shooter shall be punished for homicidal attempt even if the bullet does not hit such person. On the other hand, tort liability shall not arise in private law since there is no damage as a result of this unlawful action.

Damage is the involuntary decrease in the properties and personality values of an individual³⁴⁵. The difference between the state of the property and personality values of the individual if the damaging action did not occur and the state following the occurrence of the damaging action constitutes the damage³⁴⁶.

The sorrow and grief felt as a result of an attack to the personality of an individual is considered as moral damage³⁴⁷. Moral damage is remedied in our law in compliance with the provisions of moral compensation. The damages to occur as a result of unlawful processing of personal data are usually moral damages. a

However, an attack to the individual's personality may not always result only in moral damage. In some cases, attacks to the personality of an individual may also result in material damage³⁴⁸. Due to this reason, since the result of unlawful processing of personal data may constitute an assault to the personality rights, moral damage may arise as well as material damage. For example, the members generally give their personal information to websites in order to shop through such website or to benefit from the services of such website. Such information we share over the internet are sold to some companies by some websites and such companies send advertising mails called SPAM by using the mentioned contact information. In this case, the member may incur material damage as a result of time to be spent for deleting such mails and for the charges for internet used during such time or for not noticing an important message because of such spam messages³⁴⁹.

2.3.Causal Relationship between the Processing Activity and Damage

Appropriate causal relationship is sought for the determination of the causal relationship in the tort liability. In the doctrine, the appropriate causal relationship is

³⁴⁵ In the doctrine, some authors interpret the concept of damage within a narrower context, only as material damage. They consider the concept of moral damage as a separate concept. See: Oğuzman and Öz, Vol. II, p. 40; Tandoğan, p. 63. We shall use the concept of damage in this study within a wider context in a manner to cover the moral damage also. For the authors using the concept of damage within a wider context see: Eren, p. 545; Antalya, *Manevi Zararın Belirlenmesi*, p. 6.

³⁴⁶ Tekinay, Akman, Burcuoğlu and Altop, p. 548; Oğuzman and Öz, Vol. II, p. 39.

³⁴⁷ Antalya, *Manevi Zararın Belirlenmesi*, p. 3.

³⁴⁸ For example, an attack to the bodily integrity of a person causes such person to incur both material (art. 54 of TCO) and moral (art. 56 of TCO) damage. Moreover, art. 25 of TCC regulates that material and moral compensation may be requested by the sufferer in case of other assaults to the personality rights.

³⁴⁹ Tekil, p. 783.

the relation between an action and the damages to be incurred in the ordinary course of events as based on the life experiences³⁵⁰. For the judge to convict an individual of compensation for tort liability, it is required to establish a logical connection according to the unlawful action realized and the damage incurred as based on the ordinary course of life³⁵¹.

In assessment of the existence of an appropriate causal relationship, prediction of the damage which may occur by the offender is not important. If occurrence of such damage by such action is acceptable in the ordinary course of life, then we can say that there is causal relationship. The judge shall act as an impartial person by benefitting from his/her life experiences³⁵². The evidence of appropriate causal relationship is the responsibility of the damaged party. The judge decides whether or not there is appropriate causal relationship as based on the evidences presented.

It is not always easy to determine whether there is an appropriate causal relationship between the activity of processing of personal data and the damage. The most important reason for this is that the activity of processing the personal data is an activity that requires technique and expertise. It would be appropriate for the judge to refer to an expert concerning whether the required security measures are taken or not by the end of the processing activity, to what extent such processing is necessary or the determination of the processing means.

2.4.Fault of the Data Controller

2.4.1. Definition

Fault is the state of desiring an unlawful result or although not desiring, not showing the required care and attention in order to avoid unlawful behavior³⁵³. If the offender

³⁵⁰ Tandoğan, p. 77; Oğuzman and Öz, Vol. II, p. 45.

³⁵¹ Oğuzman/Öz, Vol. II, p. 46; Tekinay, Akman, Burcuoğlu and Altop, p. 573;

³⁵² Tandoğan, p. 8; Oğuzman and Öz, Vol. II, p. 46.

³⁵³ Oğuzman and Öz, Vol. II, p. 54; This definition is made as based on the subjective theory, one of the theories explaining fault which we also agree. This theory takes into consideration the concept of fault, the moral state, knowledge and skills, educational level of the damaging party and determines the ratio of the fault as based on the conditions which such person is in. Antalya, Vol. II, p. 26; Another opinion is the objective theory. According to the objective theory, fault is defined as the form of behavior which the order of law disapproves, does not tolerate. Tekinay, Akman, Burcuoğlu and Altop, p. 492; Tandoğan, p. 44; Antalya, Vol. II, p. 21.

acts willingly desiring the unlawful result, then there will be intention³⁵⁴, and if the offender does not desire such unlawful result, but did not show the required care and attention in order to avoid this, then there will be negligence^{355, 356}.

Both types of fault, although have different levels of severity, are the behaviors which are disapproved by the order of law. This distinction is significant with respect to the civil law liability as well as penal law³⁵⁷. In other words, negligence, which is the slightest level of fault in civil code, also gives rise to compensation. However, types of fault are important when the judge decides about the compensation. In addition, intention is required according to art. 49/2 of TCO in order to hold the offender liable in compliance with tort for unethical action.

2.4.2. Fault in the Protection of Personal Data

There is a significant difference between the EU law and Turkish law concerning whether the data controller's fault shall be sought or not in compensation of the damages to arise of unlawful processing of the personal data. Although there are provisions in the regulations of EU legislation concerning how the data controller shall be relieved of liability, the fault clause is not mentioned. However, general provisions are referred to in LPPD concerning the compensation of the damages arising of the violation of the personal data. Due to this reason, it will be beneficial to examine both conditions separately in our study.

2.4.2.1. Fault of the Data Controller in EU Law

In compliance with the art. 82/1 of GDPR, if any data subject, whose personal data are processed unlawfully, suffers any material or moral damage as a result of such

³⁵⁴ Intention is the severest degree of fault and it is divided into two categories as direct intention and indirect intention in the doctrine. Accordingly, direct intention is when the offender acts intentionally knowing the unlawful consequences. In indirect intention, the offender does not directly want the unlawful consequence. However, he/she takes the risk of realization of such consequence and performs unlawful activity. Oğuzman and Öz, Vol. II, p. 56; Tandoğan, p. 46.

³⁵⁵ Neglect is divided into two as gross negligence and slight negligence. Gross negligence is when the offender does not pay the maximum attention and care expected of such people in the same state, while performing the activity which results in unlawful consequence. Slight negligence on the other hand, is when the attention and care required to be shown by a careful and attentive person is not shown. Tandoğan, p. 48; Oğuzman and Öz, Vol. II, p. 56.

³⁵⁶ Tekinay, Akman, Burcuoğlu and Altop, p. 494; Oğuzman and Öz, Vol. II, p. 56; Hatemi and Gökyayla, p. 147.

³⁵⁷ Tandoğan, p. 46; Antalya, Vol. II, p.22.

processing activity, then he/she can claim such damages from the data controller or the data processor. In art. 82/3 of GDPR, the data controller or the data processor is required to prove that he/she is not responsible in any manner for the event giving rise to such damage in order to be relieved from the liability³⁵⁸. As it could be understood from this regulation, the data controller shall not be able to be relieved from the liability by proving that he/she does not have any fault in the unlawful processing activity³⁵⁹. In other words, if the data controller or the data processor is involved in the event giving rise to the damage, whether or not he/she is faulty, then he/she shall be held responsible for the damage³⁶⁰. Due to this reason, the data controller shall also be responsible for the unlawful processing of the data processor processing the personal data on behalf of or by the instructions of the data controller, even if the data controller is not faulty. In this case a liability heavier than the employer's liability is loaded on the data controller. According to this provision, the data controller shall be liable even if he/she proves the care he/she had shown in the selection and control of the data processor³⁶¹. Whereas, this is the evidence of salvation in the employer's liability.³⁶²

The data controller shall be required to prove either the personal data processing activity is in compliance with the Regulation or the damage has occurred outside his/her area of dominance in order to be relieved from the liability. For the data controller to prove that the damage has occurred outside his/her area of dominance, in other words, to prove that he/she is not liable for the event giving rise to the damage, he/she is required to prove that there is a third event causing the damage and that this event cannot be associated with him/herself³⁶³. In other words, the data controller can be relieved from the liability only if he/she can prove that the damage occurring is the result of an event that interrupts the causal relationship, outside his/her processing

³⁵⁸ According to art. 82/3 of GDPR; "A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage".

³⁵⁹ In the doctrine, there are authors interpreting non-inclusion of the concept of fault in the liability provisions of the Directive 95/46/EC and GDPR as "EU law makers desire to leave the decision of whether fault is a requirement of data processing activity to the discretion of the member states". Ayözger, p. 269; Özdemir, p. 215.

³⁶⁰ Alsenoy, p. 276.

³⁶¹ Alsenoy, p. 274.

³⁶² For more detailed information about the employer's evidence of salvation in employer's liability, see: Kılıçoğlu, *Genel Hükümler*, pp. 428-431; Hatemi and Gökyayla, pp. 153-155; Şahin Akıncı, p. 158; Kayıhan and Ünlütepe, p. 293

³⁶³ Alsenoy, p. 276.

activity. Even if this is not exemplified in GDPR, example is given in the 55th recital of the Directive 95/46/EC on how the data controller shall prove that he/she cannot be held responsible for the event giving rise to the damage. According to the 55th recital of the Directive, the data controller is required to prove that the damage is due to the data subject's fault or a force majeure³⁶⁴ event in order to be relieved from the liability fully or partly.³⁶⁵ As it can be understood from these examples, the data controller's civil liability in GDPR is close to the risk liability. This is because in the risk liability, there also has to be a reason that interrupts the causal relationship between the activity of the operator and the damage in order for the operator to be relieved of the liability.³⁶⁶

Another state, in which the data controller can abstain from the liability to arise of unlawful processing of the personal data, is where the data controller is the intermediary service provider. The intermediary service provider with the capacity of a data controller shall not be responsible for the unlawful processing of the personal data loaded by the third parties, on condition that the requirements of liability exemption are satisfied³⁶⁷. This state is expressed as “*This Regulation shall be without prejudice to the application of Directive 2000/31/EC³⁶⁸, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive*” in the art. 2/4 of the GDPR.

³⁶⁴ These are the events such as earthquake, avalanche or war, which occur outside the area of the person or the company, which cannot be predicted or prevented. Kılıçoğlu, *Genel Hükümler*, p. 403; Kayıhan and Ünlütepe, p. 259; In order to base on a force majeure event, the party claiming force majeure is required to prove that the counterparty encountered damage as a result of the force majeure event, that this event took place beyond his/her control and that there are no reasonable steps to be taken in order to prevent the damage that occurred as a result of such event. HFW & 20 Essex Street, *Force Majeure*, June 2018, p.4, <http://www.hfw.com/downloads/Force-Majeure-Pack-by-HFW-and-20-Essex-St-June-2018.pdf> (Access Date: 28.03.2019).

³⁶⁵ In the 55th Recital of the Directive no 95/46/EC it is stated that “*if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure*”.

³⁶⁶ For detailed information about the interruption of the causal relationship in the risk liability, see: Mesut Serdar Çekin, *6098 Sayılı Türk Borçlar Kanunu Madde 71 Çerçevesinde Tehlike Sorumluluğu*, (İstanbul: Onikilevha Yayıncılık, 2016), pp. 243-249.

³⁶⁷ Alsenoy, p. 283; For detailed information about the legal liability of the Content and Hosting Provider and the cases of exemption from such liability, see: Ümit Gezder, *İçerik Sağlayıcının ve Yer Sağlayıcının Hukuki Sorumluluğu ve Sorumluluk Muafiyeti* (İstanbul: Beta, 2017).

³⁶⁸ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), OJ. L178, 17.07.2000. Tam metin için bkz.: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML> (Erişim Tarihi: 10.02.2019).

2.4.2.2. Fault of the Data Controller in Turkish Law

In the art.14/3 of LPPD, a reference is made to the general provisions with respect to the liability of the data controller. Since there is fault liability in Turkish law as a rule³⁶⁹, in our opinion, the fault of the data controller shall be sought³⁷⁰. The art. 49 of TCO, which regulates the tort liability, and the art. 112, which regulates the liabilities arising of the breach of obligations, it is clearly understood as a rule that the fault liability as a result of material and moral damage is taken as the basis³⁷¹.

However, it should be expressed here that the LPPD imposed very strict obligations on the data controller and that the liability of the data controller approaches ordinary reason liability, which is one of the strict liability categories. When the data controller's obligation to notify the data subject during the processing of the personal data, to take any and all technical and administrative measures required for providing the data security and the data processing principles and processing conditions are taken into consideration, the data controller shall be able to be relieved of liability when he/she shows the required care and attention or when he/she proves that the damage is inevitable even if such care and attention is shown³⁷².

Another issue to be discussed concerning this subject is that whether or not the assessment of the legal liability of the data controller can be considered within the frame of the risk liability which is a state of strict liability regulated in art. 71 of TCO. As the technology develops today, information and communication sectors become the focal point of economy which bring along certain risks. Large scale companies carrying out their activities through personal data are required to provide security for the mentioned personal data. However, the production of new technological instruments may result in acquisition of the personal data by the third parties even if such sufficient security measures are taken. It is more equitable that the data

³⁶⁹ Tekinay, Akman, Burcuoğlu and Altop, p. 664; Eren, p. 513; Kılıçoğlu, *Genel Hükümler*, p. 326.

³⁷⁰ Ayözger, p. 269; Özdemir, p. 213; Taştan, p. 111; Aksoy, p. 88.

³⁷¹ Fault shall be sought in the contractual liability. However, the burden of proof for the fault is reversed. In other words, in tort liability the data subject proves the fault of the data controller, whereas if there is a legal relationship between the data subject and the data controller, the data controller shall prove that he/she does not have any fault. For detailed information, see: II. Section, 3.5.1. Proof of the Fault.

³⁷² Kılıçoğlu, *Genel Hükümler*, p. 414.

controllers keeping the data on the digital medium, processing, analyzing or transferring such data within the scope of their own activities, also undertake the protection risk of the mentioned personal data³⁷³. Due to this reason, the liability of the data controller can be considered within the scope of risk liability. This is because the risk liability is not confined to a specific area but a general provision is made in TCO.³⁷⁴ Accordingly, art. 71 of TCO can be applied for the concrete cases that provide for the conditions of the risk liability, without any need for a special provision concerning the compensation of the damages to occur as a result of the risks to arise as based on the developing technology and the necessities of the era³⁷⁵.

Due to this reason, it is required that the enterprise poses a significant level of risk for the data controller to be liable within the scope of risk liability. Two factors as objective and subjective are required to be realized in order to determine whether an enterprise poses a significant level of risk or not³⁷⁶. The enterprise's nature for causing frequent and serious damages constitutes an objective factor and inability to prevent the occurrence of the damage even if all the care is exercised by a specialist constitutes the subjective factor.

For the activities carried out by the data controller to be considered as a significant level of risk within the scope of this article shall be the determining factor in determining whether or not the data controller shall be considered within the scope of risk liability in processing of the personal data³⁷⁷. In our opinion, only the activity of processing the personal data should not bring in the risk liability. In cases where the personal data are not seen within the scope of the main activity of the enterprise, which

³⁷³ Gürpınar, p. 691. Risk liability is the liability for the damages to occur as a result of inevitable risks of some activities. Kaneti, p. 5. According to *Tekinay*; the basis of this type of liability is that the person acquiring a benefit from a thing or activity is required to bear the burden and risks of such liability. *Tekinay*, Akman, Burcuoğlu and Altop, p. 672.

³⁷⁴ Çekin, *Tehlike Sorumluluğu*, p. 123; Kılıçoğlu, p. *Genel Hükümler*, p. 469.

³⁷⁵ Senem Saraç, *Türk Borçlar Kanunu'nda Tehlike Sorumluluğu*, (İstanbul: Onikilevha Yayıncılık, 2013), p. 2. According to art. 71 of TCO, “Where damage results from the activity of an enterprise presenting a significant risk, the owner of such enterprise and, if there is one, the exploiter are severally liable for such damage.” The characteristics of an entity posing a significant level of risk are explained in art. 71/2 of TCO. Accordingly, “having taken into account the nature of the activity or material, means or powers used in it, if one infers that an enterprise is likely to cause frequent or serious damage even when all due care expected from a specialist in such activities is exercised”, then this enterprise is accepted as an enterprise posing a significant level of risk.

³⁷⁶ Çekin, *Tehlike Sorumluluğu*, p. 160-163; Saraç, p. 36; Antalya, Vol. II, p. 366.

³⁷⁷ Gürpınar, p. 691.

would not result in large data breaches, if the processing or persona data is protected within the frame of risk liability, then this shall give rise to a serious liability for the data controller. However, the activities of the enterprises such as social media websites, banks or insurance companies, which place the focus on processing and security of personal data, can be considered within the frame of the risk mentioned in art. 71 of TCO. This is because the probability of the leakage of such data without any fault on the part of such enterprises gets easier each day with the progress of technology.

Due to this reason, large number of people may be affected by the breaches to occur and this may result in large damages³⁷⁸. Even if these companies get help from the specialist in order to protect the data, they shall not be able to prevent the data violations and this shall result in serious damages in case of a breach. Accordingly, availability of a clear and explicit provision in the LPPD concerning the strict liability with respect to the legal liability of the data controller and the data processor could have ended the discussions about this issue. As a result of lack of such an regulation and lack of any decision concerning this in the Supreme Court practices, we shall examine the liability of the data controller within the frame of fault liability which is accepted as a rule.

Lack of fault clause in the art. 58 of TCO which regulates the moral compensation should not result in thinking that the moral compensation demand requires strict liability. The art. 58 of TCO, which is within the tort provisions, is a complementary of the art. 49 which is the general provision of the tort³⁷⁹. As a result, the fault shall be sought not only for the material compensation demand but also for the moral compensation demand.

³⁷⁸ For a person to be liable within the scope of risk liability, it is sufficient that a certain institution, facility or activity constitutes a special risk for the social life, without consideration of whether such person is faulty or acts contrary to the duty of care. Antalya, Vol. II, p. 359; Today, the personal data of billions of people are in the hands of ill-intentioned third parties with. Only in 2018, large companies such as *Facebook*, *Marriot Starwood Hotel*, *Quara*, *My FitnessPall* and *Google+* were required to announce that the personal data of millions of people were leaked. For the largest 21 data breaches in 2018, see: Paige Leskin, "The 21 Scariest Data Breaches of 2018", *Business Insider*, 30.12.2018; <https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#3-exactis-340-million-19> (Access Date: 23.02.2019).

³⁷⁹ Eren, p. 820.

3. CONTRACTUAL LIABILITY OF THE DATA CONTROLLER

In daily life, the individuals usually establish obligation relationship with each other as a result of social life. We establish an obligation relationship when shopping in a store, renting a house, drawing a loan from a bank or concluding a labor contract with your employer. During this relation we share our personal data with the other party of the contract. In this case, there will be a legal transaction relation between the data controller and the data subject. This makes the contract party processing the personal data, the data controller. The data controller both processes the data of the counterparty due to the conclusion of the contract or due to direct relevance with the fulfillment and processes such personal data by taking explicit consent for advertising and marketing activities.

Or in case of existence of the other lawfulness conditions stated in the LPPD, processes such personal data under a contractual relation.

The data controller shall be liable for the damage due to breach of obligations in cases such as contrary actions to the general principles of the personal data processing during such processing, non-performance of information obligation, unlawful transfer of the data to the third parties, not deleting and destroying such data when required or not providing the security for the lawfully processed data³⁸⁰.

For the data controller to be liable for the breach of obligation, first, there should be a valid contract concluded by and between the data controller and the data subject³⁸¹. This contract should impose certain primary and secondary obligations to the data

³⁸⁰ The security measures taken in order to prevent access by the third parties to the lawfully processed personal data are usually not sufficient. The recent example to this is where the user names and password combinations of the users leaked from a website are used in order to break the user data and passwords used on other websites, which is called credential stuffing attack. In these attacks the customer accounts of the companies such as *DailyMotion*, *AdGuard*, *HSBC*, *Dunkin' Donuts* and *Reddit* were illegally accessed. Catalin Cimpanu, *DailyMotion Discloses Credential Stuffing Attack*, ZDNet, 27.01.2019, <https://www.zdnet.com/article/dailymotion-discloses-credential-stuffing-attack/> (Access Date: 15.03.2019).

³⁸¹ Tandoğan, p. 415; Eren, p. 1078. Since the personal data processing activity between the social media websites and the users or the private hospitals and the patients or the banks and the customers is based on a legal relation, the compensation of the damages to occur within this frame are remedied within the frame of breach of obligation provisions.

controller and should not perform these obligations³⁸². This state constitutes the unlawful action factor of the contractual liability in tort liability³⁸³. Moreover, damage should occur as based on the breach of obligation and there should be appropriate causal relationship between this damage and the breach of obligation. Finally, the data controller is required to be faulty in his/her actions in breach of obligation, as in the tort liability. However, the burden of proof shall be reversed this time and the data controller shall be required to prove that he is not faulty for breach of obligation³⁸⁴.

3.1.Existence of a Valid Obligation Relationship

The first condition for the data controller to be liable for the breach of obligation is the establishment of a valid obligation relationship between the parties³⁸⁵. If no obligation relationship exists, there will be no non-payment of the debt by the debtor or breach of obligation. Due to this reason, there should be the constituent factors of the contract for the formation of the contract which is the largest element of the obligation relationship³⁸⁶. Moreover, the validity conditions providing for the provisions and consequences of the contract should be fulfilled.

Contract can be defined as the legal transaction established by mutual and respective expression of the parties' will in order to provide for a legal consequence³⁸⁷. The most important condition for the formation of a contract is the existence of mutual and respective expression of the parties' will³⁸⁸. Based on this, the existence of mutual and

³⁸² Tekinay, Akman, Burcuoğlu and Altop, p. 640; Tandoğan, p. 415; In other words, the contract should not be performed at all or duly. Ümit Gezder, *İçerik Sağlayıcının ve Yer Sağlayıcının Hukuki Sorumluluğu ve Sorumluluk Muafiyeti* (İstanbul: Beta, 2017), p. 102.

³⁸³ Eren, p. 1078. Tort and behaviors that breach obligation constitute the unlawful action factor of the liability law. Antalya, Vol. II, p. 12.

³⁸⁴ According to art. 112 of the TCO, the debtor is required to compensate the damages of the creditor arising of the non-performance of the obligation in full, unless the debtor proves that no fault can be imposed on him/her. According to this provision, the debtor is required to prove that he/she is not faulty due to the non-performance of the obligation in order to be relieved of the compensation.

³⁸⁵ Ayözger, p. 229; Arzu Genç Arıdemir, *Sözleşmeye Aykırılıktan Doğan Manevi Tazminat*, (İstanbul: Onikilevha Yayıncılık, 2008), p. 81.

³⁸⁶ Hatemi and Gökyayla, p. 30; Twith the progress of technology, the scope of the means used for the formation of contracts is also expanded. Now, almost all the contracts can be concluded over the internet. For detailed information about this, see. Emrehan İnal, *E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması* (İstanbul: Vedat Kitapçılık, 2005), pp. 93-164.

³⁸⁷ Kılıçoğlu, *Genel Hükümler*, p. 126; Haluk Nami Nomer, *Borçlar Hukuku Genel Hükümler*, Reviewed 14.Edition (İstanbul: Beta Yayınları, 2015), p. 31; Oğuzman and Öz, Vol. I, p. 42.

³⁸⁸ The constituent factors of a contract can be derived from the definition of contract in the art. 1 of TCO. According to this article, "Contract is formed with the mutual and respective expression of the parties' will." The first one of these declarations of intention is "proposal" and response to this proposal

respective expression of the parties' will is required in the contracts to be concluded with the data subject for the liability to arise due to breach of obligation by the data controller processing the personal data³⁸⁹. For example, if a website offering shopping over the internet processes the data such as the types of products visited, frequency of such visits during the surfing of the visitors without taking any approval of the visitors, a contract is not formed since there is no mutual and respective expression of the parties' will³⁹⁰.

For the valid formation of a contract, the factors such as compliance with the form are required to be present in cases where the factors of competency to contract, compliance with the law (mandatory provisions, public order and personal right), ethics and morals, inability for fulfillment, harmony between the will and declaration and the form of validity are sought³⁹¹. In case such factors do not exist, and there is a declaration of will, then such will shall not give rise to any legal liability³⁹².

For example, since there is no valid contract³⁹³ when a non-competent person shops in a store and the identity data and communication data of such person is taken during such shopping while issuing an invoice, the data controller shall not be liable for the breach of obligation because the data controller does not have any unlawful actions arising of the processing of the personal data³⁹⁴. The data controller is required to delete, destroy or anonymized such data since the purpose of processing disappears, even if processing is considered to be lawful. This state is clearly regulated in art. 7 of the LPPD as “*Despite being processed under the provisions of this Law and other*

is “acceptance”. The contract is formed when the proposal and acceptance meet on “fundamental points”. Hatemi and Gökyayla, p. 30.

³⁸⁹ Nomer, p. 36; Eren, p. 244; Kayıhan and Ünlütepe, p. 53; İnal, p. 94.

³⁹⁰ In such cases, the mentioned legal relation is subjected to non-existence sanction since the constituent factors of the contract do not exist. Hatemi and Gökyayla, p. 83.

³⁹¹ Kılıçoğlu, *Genel Hükümler*, p. 126; Ayözger, p. 229; Nomer, p. 56. For detailed information about the validity conditions of the legal transactions see: Oğuzman and Barlas, p. 203 ff. For detailed information about the effect of incomplete factors on the contract in case the factors of the legal transaction are not complete, see: Korkusuz and Korkusuz, pp. 35-41.

³⁹² Kılıçoğlu, *Genel Hükümler*, p. 129. For the formation of a contract, if the constituent factors exist but the validity conditions do not exist, then such contract shall be invalid. Hatemi and Gökyayla, p. 86.

³⁹³ Since the persons who do not have full competency don't have the capacity to act, the legal transactions they perform are absolutely invalid even if the counterparty acts in bona fides. Nomer, p. 65.

³⁹⁴ For detailed information about the invalidity of the contracts concluded by the parties without full competency, see: Hatemi and Gökyayla, p. 72.

related laws, personal data shall be erased, destructed or anonymized by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process”.

The art. 23 of TCC is an important provision protecting the personal rights of the right holder even if such right holder consents the violation of his/her personal rights³⁹⁵. According to this article “(1)No person may waive his/her rights and capacity to act freely even if it is in the least degree. (2) Neither a person may waive his/her freedom nor any one may impose restrictions on a person contrary to the laws and ethics.” This article protects specifically the individuals against concluding contracts against them, which damage their personality. According to this provision, all the unethical and unlawful commitments to take away an individual’s freedom to decide and his/her economic freedom shall be invalid³⁹⁶. Although the legal sanctions to be applied to the contracts concluded as contrary to the personal rights are not clearly stated in this provision, when art. 27/1 of TCO is taken into consideration, such type of contracts shall absolutely be invalid³⁹⁷. However, it can be derived from the second paragraph that such rights can be restricted on condition that they are lawful and ethical³⁹⁸.

Whether or not processing of the personal data is unlawful and unethical can be determined as based on the general principles regulated by the LPPD. This is because the processing activity that is contrary to the general principles shall be unlawful even if the explicit consent, which is the lawfulness condition, is taken. For example, during the employment interview, the employer may demand from the employee to process his/her health records or to process his/her personal data concerning employee personnel rights related to the work entries-exits or to the extent appropriate for the nature of the work. When the employee gives consent to this, then the contract shall be validly formed. However, it is different when the employer demands the periodic processing of the employee’s personal data related to his/her private life, which is not related to the work. In this case, the mentioned provisions shall be considered as

³⁹⁵ Oğuzman, Seliçi and Oktay-Özdemir, p. 220; Serozan, *Kişiler Hukuku*, p. 457; Kılıçoğlu, *Genel Hükümler*, p. 137.

³⁹⁶ Helvacı, *Gerçek Kişiler*, p. 142; Oğuzman, Seliçi and Oktay-Özdemir, p. 200.

³⁹⁷ Nomer, p. 78; Eren, p. 343; Helvacı, *Gerçek Kişiler*, p. 144; Oğuzman, Seliçi and Oktay-Özdemir, p. 215; Arıdemir, p. 83.

³⁹⁸ Concerning the consideration of some parameters when making such restrictions, see: Serozan, *Kişiler Hukuku*, p. 458; Kılıçoğlu, *Genel Hükümler*, p. 137.

invalid since they include an illegal and unethical regulation that breaches the personal rights of the employee, even if the employer gets the employee's consent during the employment interview. This state constitutes contrariety to the basic principles of bona fides rule, being relevant with and proportionate to the purpose.

The last example is when an insurance company concludes an agreement without making the required notification before the conclusion of the insurance contract with respect to the data to be processed, this can be a reason for cancellation since it will give rise to a disagreement between the will and the declaration of will even if the data subject's declaration of will is formed³⁹⁹. In this case, the fault and fraud provisions in the general provisions can be referred to⁴⁰⁰. As a result, a valid contract still does not exist.

In short, since an obligation relationship cannot be established in cases when the contract is not formed or when formed but is considered to be absolutely invalid, there shall also be no breach of obligation⁴⁰¹. Due to this reason, legal liability shall not exist due to noncompliance with the contract⁴⁰². If the data subject trusts the data controller concerning the formation of the contract and as a result, damage arises, then such damage can be compensated within the frame of culpa in contrahendo liability⁴⁰³.

3.2. Breach of Obligation by the Data Controller

Breach of obligation is the state of non-fulfillment of the obligation, non-performance of the obligation. In other words, breach of obligation can be defined as the state in which the debtor does not perform his/her obligations in compliance with the contract that are required to be performed as a result of an obligation relationship. In order to determine the liability due to the breach of obligation, first it is required to determine the obligations which the debtor shall undertake as a result of a legal relation.

³⁹⁹ In cases where there is no will or declaration of will, the constituent factors of the contract also do not exist and as a result these are subject to non-existence sanction. However here, there is non-compliance between the will and the declaration. Şahin Akıncı, p. 87; Hatemi and Gökyayla, p. 89; Yıldırım, p. 117.

⁴⁰⁰ Ayözger, p. 229.

⁴⁰¹ Eren, p. 1061.

⁴⁰² Ayözger, p. 230; Eren, p. 1038;

⁴⁰³ Ayözger, p. 230.

3.2.1. Obligations Arising of an Obligation Relationship

Obligation relationship is the legal relation that gives rise to the debts and receivables between the creditor and debtor⁴⁰⁴. The most important characteristic of an obligation relationship that differentiates it from the other legal relations is that the parties of this type of relation are limited and definite. In other words, there is one or more debtor against one or more creditors that constitute the parties of this type of relation⁴⁰⁵. As a rule, the obligation relationship gives rise to a right for one party of the relation whereas it gives rise to an obligation for the other party. Or, one party may be the debtor and the creditor at the same time⁴⁰⁶. There are some obligations arising of the obligation relationship for the debtor. If these obligations are not fulfilled, the compensation liability of the debtor may arise. These are divided into two categories as performance obligations and secondary obligations⁴⁰⁷.

3.2.1.1. Performance Obligations

Performance obligations are the behaviors or benefits in the form of giving, performing or not performing, which constitute the basic subject of the obligation relationship which the debtor is required to perform for the creditor⁴⁰⁸. Performance obligation is divided into two as the primary performance obligation and secondary performance obligation⁴⁰⁹. The primary performance obligations are the obligations which constitute the principal obligation of the debtor in an obligation relationship which form the main frame of the contract, determine the type, kinds and features of the contract⁴¹⁰. The fulfillment of the primary performance obligations as independent of the other obligations arising of the obligation relationship can be litigated⁴¹¹. In a sales contract, transfer by the seller of the ownership and possession of the product sold, and payment by the buyer of a price in consideration of this transfer or processing of the personal data by the data processor under a personal data processing contract and

⁴⁰⁴ Eren, p. 22; Nomer, p. 13; Osman Gökhan Antalya, *Borçlar Hukuku Genel Hükümler*, Vol. I, 2.Edition (İstanbul: Legal Kitabevi, 2018), p. 10; Kılıçoğlu, *Genel Hükümler*, p. 1.

⁴⁰⁵ Kılıçoğlu, *Genel Hükümler*, p. 10; Eren, p. 27.

⁴⁰⁶ Nomer, p. 13; Kılıçoğlu, *Genel Hükümler*, p. 3.

⁴⁰⁷ Eren, p. 29.

⁴⁰⁸ Antalya, Vol. I, p. 13; Kılıçoğlu, *Genel Hükümler*, p. 3.

⁴⁰⁹ Ayözger, p. 230; Eren, p. 31.

⁴¹⁰ Eren, p. 31; Antalya, Vol. I, p. 13;

⁴¹¹ Antalya, Vol. I, p. 14

the obligation of the data controller to pay a fee in consideration of this are the examples to the primary performance obligations⁴¹².

Secondary performance obligations are the obligations outside the primary performance that constitute the principal purpose of the contract, which impose secondary obligations on the debtor, of which the fulfillment can be litigated independently since these are independent with respect to their purpose and content⁴¹³. These obligations do not determine the type and features of the contract like the primary performance obligations, but they constitute a secondary obligation providing the full and accurate realization of the purpose expected of the contract. For example, an obligation relationship is established between the user and the service provider when subscribing to a social media website. In this obligation relationship, the personal data shared by the user cannot be deleted without the consent of the user. This is because the protection of data is the secondary performance obligation of the service provider.

These obligations can arise of the law⁴¹⁴, as well as of the parties or the rules of bona fides as based on the principle of freedom of contract⁴¹⁵. Examples from the law concerning the secondary performance obligation specifically regulated can be given as; the obligation of the data controllers to erase the personal data which are lawfully processed in case the reasons requiring the processing disappears (art. 7 of LPPD), data controller's obligation to inform the data subject (art. 10 of LPPD), or the obligation of the data controller to take all the technical and administrative measures in order to provide the data security (art. 12 of LPPD). If the secondary performance

⁴¹² Taştan, p. 118.

⁴¹³ Eren, p. 33; Antalya, Vol. I, p. 14.

⁴¹⁴ In the law, the obligations constituting the primary performance obligation for some contracts can be regulated in another contract as the secondary performance obligations with the wills of the parties. Such type of contracts should not be confused with mixed contracts. In mixed contracts, the primary performance obligations of the different types of contracts are formed by provision within a contract by preserving their own qualities (primary obligation). However, in the other case, the primary performances are fixed and the obligation constituting a primary performance obligation in another contract is regulated as a secondary obligation, subject to the primary performance obligation. And the types of the contracts are formed by the primary performance obligations. Eren, p. 33.

⁴¹⁵ Antalya, Vol. I, p. 14; for detailed information about the sources occurrence of the secondary performance obligations see: Eren, pp. 34-37.

obligations are not fulfilled, the creditor may file an action for fulfillment and may have the damage compensated in compliance with the articles 112 or 125 of TCO.

3.2.1.2.Secondary Obligations

The obligations arising of an obligation relationship are not only the primary and secondary performance obligations. The obligation relationship also imposes some secondary obligations on the parties, arising of the rule of bona fides regulated in art. 2/1 of TCC.⁴¹⁶ Since the secondary obligations depend on specifically the primary performance obligation, they cannot be the subject of a separate action and its fulfillment cannot be demanded independently⁴¹⁷. However, if the debtor causes damage by his/her actions that breach the secondary obligation, then the creditor may demand the compensation of the damage to occur. As a result, it can be stated that the secondary obligations enable the creditor to file only an action for compensation, not an action for performance.

Secondary obligations are divided into two within themselves as “secondary obligations serving the fulfillment” and “protective secondary obligations”. Secondary obligations serving the fulfillment are the obligations that arise of the rule of bona fides which provides the realization of the purpose of the contract by serving the fulfillment of the primary performance constituting the primary obligation of the contract, in a full and accurate manner⁴¹⁸. The secondary obligations serving the fulfillment come to the foreground at the preparation stage or during the fulfillment of the performance⁴¹⁹. For example, the collection of the data of the members by the social media websites when concluding the social media service contract in order to offer service to such members and the obligation of establishing the infrastructure to provide the analysis of such data in a specific manner are the secondary obligations serving the fulfillment. Accordingly, the service provider shall be able to offer quality service to the members. If another example concerning this issue is to be given, the data

⁴¹⁶ Supreme Court, 9.CC., 01.02.2010, M. 2009/13572, 2010/1816- Legalbank Elektronik Hukuk Bankası, (Access Date: 10.10.2018); Supreme Court, 19.CC., 20.012014, M. 2013/16574, D. 2014/1532 – Legalbank Elektronik Hukuk Bankası, (Access Date: 10.10.2018).

⁴¹⁷ Eren, p. 37; Antalya, Vol. I, p. 15.

⁴¹⁸ Antalya, Vol. I, p. 15; Eren, p. 38.

⁴¹⁹ Eren, p. 38.

controller's obligation to cooperate with the data subjects for the protection of the data is also a secondary obligation.

The parties have some obligations against each other since there is a social contact between the parties during a contractual relation. These obligations called protection obligations can be applicable before the formation of the contract or during the fulfillment of the performance and even following the termination of the contract⁴²⁰. For example it is a protective secondary obligation for a bank to take the technical measures within its own system in order to provide secure protection of the customers' data.

In some cases, although the obligation relationship between the parties ends, the obligations of the parties to protect each other continue. Specifically, the "loyalty obligation" of the parties to each other sets an example to the post-contract protection obligations⁴²¹. Accordingly the data controller processing the personal data under a contractual relation should delete such data following the termination of the contract and should not share these with a third party. This state regulated in art. 12/4 of the LPPD. According to this provision, "*The controllers and processors shall not disclose the personal data that they learned to anyone in breach of this Law, neither shall they use such data for purposes other than processing. This obligation shall continue even after the end of their term*". In such cases, application of the tort provisions is not satisfactory due to the damage to the values such as equity, relation of confidence and the rules of bona fides⁴²². Accordingly, the application of contractual liability is the opinion that is accepted in the doctrine⁴²³.

3.2.2. Data Controller's Activities that Breach the Contract

We mentioned that the performance obligations and secondary obligations are included within the scope of the liability arising of the contract. The debtor is required to act in compliance with these obligations and not to violate these. Violation of these obligations shall give rise to actions that breach the contract. As a result, it can be

⁴²⁰ Nomer, p. 14; Eren, p. 40.

⁴²¹ Eren, p. 42.

⁴²² Antalya, Vol. I, p. 17; Eren, p. 42.

⁴²³ Eren, p. 42.

stated that the violation of the performance obligations and the secondary obligations shall constitute the basis for the liability arising of the contract⁴²⁴. Accordingly, if the data controller does not duly carry out the performance obligations or the secondary obligations, this shall give rise to the contractual liabilities of the data controller.

The data controller may not perform such obligations in various cases. These are impossibility of fulfillment of the obligation, non-fulfillment in full or as required or the default of the debtor. Non-fulfillment in full or as required is an upper concept and what should be understood from this is the bad fulfillment or the violation of the secondary obligations⁴²⁵. In such cases, TCO gives some rights to the creditor. Articles 112 and 116 of TCO shall be referred to if the obligation is not fulfilled in full or as required and article 117 ff. of TCO shall be referred to if there is any default. In cases of breach of contract, the debtor is required to remedy the damage to be incurred by the creditor. The cases of breach of obligation arising of the data processing in the contracts in which the personal data are processed usually cover the cases of non-fulfillment of the obligation as required.

Duly fulfillment can be defined as full and accurate performance of the mentioned performance in compliance with the obligation relationship⁴²⁶. In case the performance fulfilled by the debtor does not comply with the qualities of the performance decided in the contract, then it shall be considered as not duly fulfilled. Within this context, the state of not fulfilling duly can be in the form of non-fulfillment of the performance obligations by bad fulfillment or in the form of breach of any of the secondary obligations. In case the data controller does not fulfill the obligations arising of the contract, during the processing of the personal data or during the protection of such data, as explained above, then he/she shall be considered as not fulfilling the performance duly.

Mentioned breach of obligation can be performed by the debtor or any third party liable for his/her actions⁴²⁷. For example, breach of obligations in protection of the

⁴²⁴ Arıdemir, p. 85; Eren, p. 1062.

⁴²⁵ Eren, p. 1053.

⁴²⁶ Eren, p. 1072.

⁴²⁷ Eren, p. 1052.

personal data can be made by the data controller who is a party to the contract or an employee of the data controller or the data processor.

3.2.2.1. Breach of Contract if Processing of Personal Data is a Performance Obligation

The action of processing or protection of personal data appears as a performance obligation in some contracts. In this case, the contractual liability of the data controller arises and action for both fulfillment and compensation can be filed. For example, a contract can be concluded with a third party in order to keep and protect the data of the customers or the employees lawfully processed by the data controller. In this case, the primary obligation of the other party of the contract who is in the position of data processor shall be to store such data and prevent their acquisition by the third parties. However, if such data stored are deleted, erased, then the inability to perform for the data processor shall arise. Accordingly, there shall be breach of obligation. The data controller cannot demand specific action for fulfillment and can file a compensation case against the data processor. Moreover, the data subject shall be able to file a case against both the data controller and the data processor for the compensation of the damages to occur as a result of erasure or destruction of such data. This state is expressed as *“In case of the processing of personal data by a natural or legal person on behalf of the controller, the controller shall jointly be responsible with these persons for taking the measures laid down in the first paragraph”* in art. 12/2 of LPPD.

Another example of processing of the personal data being a performance obligation is the processing obligation of *“Family Locator”* family tracking application, the location data of the users in compliance with the contract concluded with the users.⁴²⁸ This application enables the family members downloading such application to see the real-time location data of each other and accordingly the spouses can easily track each other and the parents can easily track their children. The processing of location data is a primary performance obligation in the contract concluded by and between the service provider offering this service and the user. Also, providing security for such data shall constitute a secondary performance obligation for the service provider, who has the

⁴²⁸For the mentioned application see: https://play.google.com/store/apps/details?id=com.life360.android.safetymapd&hl=en_US (Access Date: 02.03.2019).

capacity of a data controller, and the mentioned company shall directly be liable for unauthorized access of other to such data ⁴²⁹. In this case, if there is any violation concerning the processing and protection of personal data constituting the subject matter of the contract, then the members of the social media website can file action for compensation in order to remedy the damage incurred by them⁴³⁰.

3.2.2.2. Breach of Contract if the Performance of Processing or Protection of Personal Data is a Secondary Obligation

In an obligation relationship, another benefit of the creditor in addition to the performance benefit is the protection benefit. Each party of the contract has the obligation of preventing the occurrence of any damage to the properties and personal values of the other party during the fulfillment of the performance or due to fulfillment⁴³¹. This obligation which is called protection obligation constitutes another type of not fulfilling duly. The data controller in the position of the debtor is required to protect the rights of the creditor, other than the benefits expected of the contract such as the real rights and personal rights of the creditor. In case of leakage due to unlawful processing of the personal data or insufficient security measures for the processed personal data, this shall constitute a direct attack to the personal rights of the data subject and such cases shall cause the data controller to violate the protection obligation.

For example, let's assume that a private hospital issues the medical history of the patients in its system order to offer better service. The treatment services carried out by the hospital in order to cure the patients constitute a performance obligation, whereas processing of the past health problems of the patients in order to offer better

⁴²⁹ Concerning this application's leaving real time location data of more than 238,000 users unprotected and accordingly enabling the third parties to access such data, see: Zack Whittaker, "A family tracking app was leaking real-time location data", *TechCrunch*, 23.03.2019, <https://techcrunch.com/2019/03/23/family-tracking-location-leak/> (Access Date: 24.03.2019).

⁴³⁰ In the recent periods, the news that the personal data of the users are not sufficiently protected by Facebook disturbs the users. A recent example to this is the news that data were leaked as a result of hacker attack that affected 50 million users of Facebook on September 20, 2018. Accordingly, the hackers took advantage of the security vulnerability of "view as" feature of Facebook and stole the access tokens having the function of a digital key. As a result, unidentified people had the access any account they desire without logging on. <https://www.ntv.com.tr/teknoloji/50-milyon-facebook-hesabina-saldiri,aSPJs7bAmEWYM2s77zQiYQ> (Access Date:27.11.2018)

⁴³¹ Aridemir, p. 89; Eren, p. 1077.

service and accurate diagnosis can be considered as a secondary obligation serving the fulfillment. However, taking the measures to prevent the access of the third parties to such lawfully processed data or protection of such data in a secure manner is the result of “*protection obligation*”. If such data are leaked or deleted as a result of any security vulnerability, it shall be accepted that an attack is made to the personal rights of the patients and the protection obligation shall be violated⁴³².

Telecommunication company offering electronic communication service is able to listen to the telephone calls of its customers and record them, thanks to the technical infrastructure it possesses. Due to this reason, the company, which is in the position of data controller, should protect the confidentiality of these calls directly concerning the private life of the customer, who is in the position of data subject, within the scope of duty of loyalty⁴³³. Selling such personal data acquired from these calls to a third party in consideration of a payment shall constitute breach of obligation and the company shall be held liable for the damages to arise as a result.

The data controller’s liability to the data subject, who is the counterparty of the contract, shall continue even after the lawful processing of the personal data. For example, a bank, which is in the position of data controller, is under accountability obligation upon the demand of its customer about the personal data which are lawfully processed during a processing activity carried out in the banking sector. This state is the requirement of the rule of bona fides as well as it is a right given in art. 11 of the LPPD to the data subjects. Accordingly, the bank in its capacity as the data controller is under the obligation of accounting if demanded by the customer, whether or not

⁴³² Each day, a new one is added to the violations concerning the security of the personal data processed over the internet medium. Again in the recent periods, the data such as the location of the users, device type, IP address, URL of the files logged on are leaked due to the security vulnerability of the web log database of *Kanopy* website, which is one of the free movie websites. With such information, it is possible to identify the identities of the data subjects and which types of videos they watch as online. Simon Cohen, “Kanopy Privacy Breach Reveals Which Movies Members Have Been Streaming”, *Digital Trends*, 22.03.2019, <https://www.digitaltrends.com/home-theater/kanopy-streaming-data-breach/> (Access Date: 24.03.2019). Again, in the recent periods, Facebook confessed that its employees can easily access the passwords of 200 million to 600 million users since these were registered in plain text format, without encryption. This state prepared the grounds for about 20 thousand company employees to access such user passwords easily. Lily Hay Newman, “Facebook Stored Millions of Passwords in Plaintext- Change Yours Now”, *Wired*, 21.03.2019, <https://www.wired.com/story/facebook-passwords-plaintext-change-yours/> (Access Date: 24.03.2019).

⁴³³ Ayözger, p. 231.

their personal data are processed, if processed, the required information, the purpose of processing and whether or not they are used appropriately for this purpose, to whom and for which purpose such data are transferred in the country or abroad.

One of the behaviors that violate the secondary obligations serving the fulfillment the most in practice is the violation of the obligation to inform⁴³⁴. For example, in compliance with an insurance contract concluded with the client, an insurance company has undertaken to pay the healthcare expenses of the client which may be incurred in future. Although the insurance company informed that the personal data shall be processed while concluding the contract, it did not inform the client what these data are, or for which purpose and based on which grounds they shall be processed or whether or not these shall be transferred to the third parties. In this case, the data controller processing the data such as health data, family relations, work position of the client did not perform the required obligation to inform and this gives rise to not fulfilling duty due to the breach of secondary obligation⁴³⁵.

3.3.Damage to Arise due to Breach of Contract

Another element for the liability to arise of breach of obligation is the occurrence of damage against the creditor⁴³⁶. In general, the damage to arise of breach of obligation is the decrease that results as contrary to the creditor's will, in the benefits of the

⁴³⁴ According to a decision of the Supreme Court; it is stated that “*with respect to the vehicle in question, the authorized dealer did not inform the claimant company duly in compliance with the Law and the rule of Bona Fides (art. 2 TCC) whether VAT shall be set off or not and accordingly, acted contrary to the disclose obligation, which is a secondary obligation of the sales contract and violated the contract*”. Supreme Court, 19.CC., 20.01.2014, M. 2013/16574, D. 2014/1532 – Legalbank Elektronik Hukuk Bankası, (Access Date: 10.02.2019).

⁴³⁵ This state is separately considered in the LPPD and the obligation to inform the data subject during the processing of the personal data is imposed on the data controller. As a result, during a contractual relation the boundaries are drawn with respect to the issues which the data controller or the data processor should inform the counterparty. The art. 10 of the LPPD, with the title Obligation of Controller to Inform imposes an obligation to inform as “*the controller or the person authorized by him/her is obliged to inform the data subjects about the identity of the controller and of his/her representative, if any, the purpose of data processing, to whom and for what purposes the processed data may be transferred, the method and legal reason of collection of personal data, other rights referred to in Article 11*”. In case of breach of obligation to inform, an administrative fine of 5.000 to 100.000TL is to be paid.

⁴³⁶ Tandoğan, p. 424.

creditor which are protected lawfully, as a consequence of the breach of contract⁴³⁷. In this type of liability, the damage is divided into two as material and moral damage⁴³⁸.

The cases to cause material damage occur as the violation of the personal values or the property values. Since the personal values are among the moral rights, material damage may occur as a result of violation of such rights even if these do not have a material value⁴³⁹. For the violation of personal values to result in material damage, the attack realized on the personal value is required to have a negative effect on the properties of the person⁴⁴⁰. Unlawful processing of the personal data causes the violation of the personal values of the person. As a result of this, if there is any negative effect on the properties of the data subject, then the data subject may claim the material damage. In practice, it is very rare that a person incurs material damage due to the unlawful processing of his/her personal data. For example, if the hotel records of an actor playing a religious character in a religious movie, where he went with his girlfriend, are leaked to the press by the hotel management, the damages incurred due to the termination of his contract with the production company, the damages due to not extending a credit to a person based on unlawful processing of the personal data⁴⁴¹ are included in this category. Or if a bank does not take adequate measures in order to protect the account details of the customer, and if such account of the customer is accessed and used by the third parties, the money in the account are transferred to a third party beyond the customer's knowledge, then the material damage to occur is examined within this frame⁴⁴². Moral damage is the decrease in the lawful values

⁴³⁷ Eren, p. 1078. Korkusuz and Korkusuz, p. 41.

⁴³⁸ Tandoğan, p. 424.

⁴³⁹ Oğuzman, Seliçi and Oktay-Özdemir, p. 262.

⁴⁴⁰ Eren, p. 1079.

⁴⁴¹ Çekin, *Kişisel Verilerin Korunması*, p.102.

⁴⁴² According to the decision of the Supreme Court, illegally drawn money directly is in the nature of the bank's damage and the depositor's claims from the bank continue as it is. Due to this reason, it can set this off from the receivables of the account holder in compliance with concurrence negligence provisions to the extent it is proved that the depositor is faulty in creation of the mentioned damage. Supreme Court, 11.CC., 03.03.2011, M.2009/8730, D.2011/2237- Legalbank Elektronik Hukuk Bankası, (Access Date: 15.03.2019). Accordingly, if it is proven that the data subject is not faulty in protection of the personal data or if his/her fault is not proven, then the banks shall presumptively be in breach of obligation and shall directly be liable of the damage to occur. In another Supreme Court Decision concerning this issue; "...the money of the claimant is transferred from one account to another by a transaction realized against the bank and this state shall not release the defendant bank from its obligation to return the deposit taken and the defendant bank which has the burden of proof, could not prove that the password and cipher given to the claimant is acquired as based on the fault of the

constituting the personality of a person, which occur as involuntarily⁴⁴³. Personal values are all the values arising of a person's being an individual, which are protected by the law⁴⁴⁴. The values of such life, body integrity, honor, freedom, health create the personal values whereas the personal data are also considered to be included within this frame. Sometimes the moral damage to occur is a result of breach of contract⁴⁴⁵.

However, it should be underlined here that moral compensation cannot be claimed in every breach of obligation. In order to claim moral compensation, there should be an illegal attack on the personal rights and a moral damage should arise as a result of this attack. Since processing of personal data unlawfully may violate the values such as the privacy of the private life, individual's right to determine own destiny or the human dignity, which are the concrete appearances of personal right, the moral damage shall also be taken into consideration in the contractual liability of the data controller.

3.4.Relation between the Breach of Obligation and Damage (Appropriate Causal Relationship)

For the occurrence of the liability of the data controller arising of the contract, there should be an appropriate causal relationship between the violation of contractual obligations and the damage to occur. Ordinary course of events and general life experiences are benefitted from in determination of this relationship. If the breach of obligation according to the ordinary course of events and the general life experience is appropriate to cause the damage in the event in question, then there is appropriate causal relationship⁴⁴⁶. In the example given above, there is an appropriate causal relationship between the action of leaking the hotel records of the actor playing a religious role, who stayed in the hotel with his girlfriend, to the press by the hotel

claimant. The defendant did not obligate the use of means which would provide the security for itself and the customers in internet banking, and left this to the initiative of the claimant in the case in question, which was the main factor in the occurrence of the damage, accordingly it is evident that the defendant bank is solely liable for the damage". Supreme Court, 11.CC., 14.03.2011, M.2009/9801, D.2011/2673- Legalbank Elektronik Hukuk Bankası, (Access Date: 15.03.2019).

⁴⁴³ According to Eren, who supports the objective opinion with respect to the moral damage, the moral damage is the decrease in the legal values constituting the personalith of a person, which occur beyond such person's will. Eren, p. 556; Antalya, *Manevi Zararın Belirlenmesi*, p. 6.

⁴⁴⁴ Oğuzman, Seliçi and Oktay-Özdemir, p. 172.

⁴⁴⁵ For the decisions causing the violation of personal rights as a result of breach of obligation see: Supreme Court, 13. CC., 30.06.2011, M. 2011/2670, D. 2011/10460; Supreme Court, ACC., 6.11.2013, M. 2013/3-56, D. 2013/1525- Legalbank Elektronik Hukuk Bankası, (Access Date: 16.03.2019).

⁴⁴⁶ Tandoğan, p. 430; Eren, p. 1086.

management and the termination of the contract between the actor and the production company.

3.5.Data Controller's Fault

Fault liability is sought as a rule in the contractual liability⁴⁴⁷. This condition is understood from the provision of the art. 114/1 of TCO which is as “*is generally liable for any fault*”. Moreover, according to art. 112 of TCO, the debtor is required to compensate the damages of the creditor, arising of the breach of obligation, as long as he/she does not prove that he/she is not faulty. Due to this reason, fault shall be sought as a principle in the liability arising of the contract concluded between the data controller and the data subject.

Fault in the contractual liabilities can be defined as the preventable action of the debtor that breaches an obligation⁴⁴⁸. In other words, it is the deviation of the debtor from the behaviors exhibited by a reasonable and honest debtor in his/her social and professional medium, when fulfilling his/her obligations, in a manner not approved by the law⁴⁴⁹. When compared with a standard person performing similar work, that person's inattentive behavior presumptively reveals the fault.

In the contractual liability is divided into two categories, just like in tort liability, as intention for fault and negligence. Intention is the debtor's non-fulfillment of the primary and secondary obligations arising of a legal transaction, by planning or desiring or by risking the consequences⁴⁵⁰. For example, if the employee of a shoe store also takes the contact number for advertising purposes while taking the identity and address data of the customer while issuing an invoice, and does not notify the counterparty of the contract about this processing, then this shall be an unlawful processing. Negligence can be defined as not paying the attention and care required to be paid under the same conditions when compared with other people of the same professional group or in the same position, although the debtor does not desire to neglect the contractual obligations⁴⁵¹. As an example to this, let's think that the same

⁴⁴⁷ Oğuzman and Öz, Vol. I, p. 404; Eren, p. 1086; Başak Baysal, *Zarar Görenin Kusuru-(Müterafik Kusur)*, (İstanbul: Onikilevha Yayıncılık,2012), p. 284.

⁴⁴⁸ Tandoğan, p. 416.

⁴⁴⁹ Eren, p. 1087.

⁴⁵⁰ Oğuzman and Öz, Vol. I, p. 405.

⁴⁵¹ Eren, p. 1088.

employee of the shoe store stores such personal data of the customer processed lawfully in his/her own software program. However, when we consider that he/she does not have the adequate measures to prevent the access of the third parties to such data and that he/she does not take the required measures, then there is negligence here. This is because another average shoe store in the same sector shall be able to pay the required care and attention for the security of its customers.

3.5.1. Proof of the Fault

The most important difference of the contractual fault from the fault in tort liability is in the issue of proof. According to art. 6 of TCC “*each party is required to prove the existence of the facts on which such party basis his/her rights*”. Due to this reason, the general principle in Turkish Private Law is that the person claiming that another person is faulty is required to prove the fault of such person, unless there is a contrary legal provision in the proof of the fault. Accordingly, the injured party is required to prove the fault of the damaging party in tort liability. However, in contractual liability this rule is reversed. While the creditor is required to prove that the debtor is faulty for his/her behaviors that are in breach of obligation, art. 112 of TCO imposes the burden of proof on the debtor that no fault can be attributed to the debtor due to his/her behaviors that constitute a breach of obligation⁴⁵². In other words, the debtor shall not be released of the contractual liability until he/she proves that he/she is not faulty in the breach of obligation⁴⁵³.

In this case, the data controller is required to bring the evidence of his/her no-fault state or evidence of salvation in order to prove his faultlessness. Bringing such evidences is very difficult for the data controller. The data controller can be released of liability in case he/she proves that the contract is violated as a result of extraordinary events. What is meant by extraordinary external events are force majeure events and the gross negligence of the data subject or a third party that interrupt the causal relationship.⁴⁵⁴. For example, if the personal data lawfully processed by the data controller are acquired by a third party, although the data controller fully carried out

⁴⁵² Tandoğan, p. 62; Baysal, p. 285; Korkusuz and Korkusuz, p. 65.

⁴⁵³ For the discussions on debtor’s evidence that he/she is not guilty concerning the proof of burden in contractual liability approaches the debtor’s liability to strict liability, see: Baysal, pp. 285-289.

⁴⁵⁴ Eren, p. 1092.

his/her obligations stated in the articles 10 and 12 of the LPPD, then there will be no fault on the part of the data controller. Breach of obligation shall take place due to the gross negligence of the third party and the data controller shall be released from liability for the breach of obligation upon proving that he/she had paid due care and attention in fulfilling the legal obligations⁴⁵⁵.

Art. 112 of TCO which reverses the burden of proof is not a mandatory provision, and if the parties agree among themselves, it is possible to impose the data controller's burden of proof for the fault on the data subject⁴⁵⁶.

3.5.2. Non-liability Agreement in the Processing of Personal Data

The agreements to be concluded by the parties which narrow down the liabilities of the debtor are called non-liability agreements⁴⁵⁷. When the art. 115/1 of TCO is interpreted reversely, the parties may add a clause to the agreement that the debtor shall not be liable for the breach of obligation in case of slight negligence⁴⁵⁸. Accordingly, the debtor shall only be liable for gross negligence and shall not be liable for the damages to occur as a result of slight negligence⁴⁵⁹.

Within the scope of the protection of personal data, there is no explicit provision in the LPPD that a non-liability agreement cannot be concluded by and between the data subject and the party of the agreement which has the capacity of a data controller, with respect to the personal data processing activity. However, the obligations of the data controller stated in art. 12, the main principles for processing the personal data and lawfulness conditions are taken into consideration, it is apparent that the data controller shall be liable even for the slight negligence. The regulations in the law are mandatory provisions and when the non-liability agreement to be concluded by the parties is

⁴⁵⁵ Oğuzman and Öz, Vol. I, p. 408.

⁴⁵⁶ Oğuzman and Öz, Vol. I, p. 404

⁴⁵⁷ Nilgün Başalp, *Sorumsuzluk Anlaşmaları* (İstanbul: Onikilevha Yayıncılık, 2011), p. 17; Oğuzman and Öz, Vol. I, p. 409.

⁴⁵⁸ Tandoğan, p. 417.

⁴⁵⁹ TCO provided two limitations for the agreements concerning the non-liability of the debtor due to the slight negligence. These are the cases in which the debtor has a service agreement with the creditor and the cases in which a service, profession or art requiring specialization can only be carried out with the permission to be given by the law of the authorities. For detailed information, see: Başalp, *Sorumsuzluk Anlaşmaları*, p. 249 ff.; Oğuzman and Öz, Vol. I, pp. 412-413.

considered within this frame, it shall definitely be invalid according to art. 27/1 of TCO⁴⁶⁰.

3.5.3. Strict Liability of the Data Controller

As in the tort liability, there are some cases also in the contractual liability in which fault is not sought⁴⁶¹. The most important one is being liable for the actions of the assisting persons regulated by the art. 116 of TCO According to this article, the debtor may use some people lawfully in order to fulfill the debt. The debtor shall have strict liability for the damage to be incurred by the creditor when they fulfill the debt⁴⁶². For example, the data controller may request the data processor, who has the capacity of another natural person or legal person, to process and store the data of the data subject. In this case, the data control shall have strict liability for the damages arising of the violation with respect to data processing performed by the data processor.

For example, when an employee working at the financial affairs department of a company transfers the names surnames of the employees, their identification numbers and account data in consideration of a payment to another company performing in the same sector, then liability shall arise for the unlawful processing of the personal data of the mentioned company employees⁴⁶³. Accordingly the capacity as the data controller continues in compliance with the provisions of LPPD and shall be liable for not providing the security of the mentioned data.

However, it should be expressed that if the data controller is a legal person, the actions carried out by the organs of the legal person both for the fulfillment of the debt and the use of right, are not assessed within this frame⁴⁶⁴. This is because the personal data processing activity carried out by the organs of the legal person is considered to be the

⁴⁶⁰ For detailed information about the effect of the invalidity of the non-liability agreements on the main agreement, see: Başalp, *Sorumsuzluk Anlaşmaları*, p. 383 ff.

⁴⁶¹ Liability for the actions of assisting persons, fulfillment of monetary debt, liability of the debtor in case of defective fulfillment or the liability of the debtor concerning the debtor's default are the examples to the strict liability conditions in contractual liability. Baysal, p. 285.

⁴⁶² Eren, p. 1093; Oğuzman and Öz, Vol. I, p. 416; Baysal, p. 285.

⁴⁶³ For the decision concerning the employee accessing the identity information of the other employees working in financial works and sending such information to a third party, and accordingly causing contrary actions of the employer to the provisions of the LPPD, see: Supreme Court, 22. CC., 28.05.2018, M. 2017/13673, D. 2018/13196 (Legalbank Elektronik Bilgi Havuzu)

⁴⁶⁴ Oğuzman and Öz, Vol. I, p. 420.

activity of the legal person. Due to this reason, the legal person itself is liable directly for the damage to arise of such activities.

4. CULPA IN CONTRAHENDO LIABILITY OF THE DATA CONTROLLER

4.1. Culpa in Contrahendo Liability in General

Culpa in Contrahendo (*CIC*) liability⁴⁶⁵, defines the liability to arise of the damages to occur as a result of the actions of the negotiators of the contract, which are contrary to the rule of bona fides, during the contractual negotiations⁴⁶⁶. In other words, compensation of the damage to arise as a result of faulty actions of any of the parties which are contrary to the rule of bona fides regulated by the art. 2 of TCC, during the pre-contractual negotiations, results in *CIC* liability⁴⁶⁷.

CIC liability, which constitutes a special outlook of the rule of bona fides regulated by the art. 2 of TCC, emerges during the negotiations before the contract. Accordingly, the rule of bona fides imposes some obligations on the parties during pre-contractual negotiations⁴⁶⁸. Non-compliance of the parties with the obligation of protection of and providing information to each other during these negotiations, supplying faulty information about the content and conditions of the contract or not showing the due care and attention in order to hold the personal and property values harmless or deceptive actions performed in order to achieve the formation of the contract, being in the wrong by his/her own faults at a level requiring the cancellation of the contract are

⁴⁶⁵ Culpa in Contrahendo liability was first claimed by the German legist Jhering in 1861. In an article Jhering published on this date, he defended the compensation to be claimed from the party causing the damage to arise due to non-formation of the contract as a result of faulty behaviors during the contractual negotiations or causing its invalidity. Gezder, *Culpa in Contrahendo Sorumluluğu*, p. 1. The term Culpa in Contrahendo is a term in Latin and it means fault in contractual negotiations. Oğuzman and Öz, V. I, p. 478; Huriye Reyhan Demircioğlu, *Güven Esası Uyarınca Sözleşme Görüşmelerindeki Kusurlu Davranıştan Doğan Sorumluluk* (Ankara: Yetkin Yayınları, 2009), p. 41; Culpa in Contrahendo shall be referred to as “*CIC*” hereinafter.

⁴⁶⁶ Gezder, *Culpa in Contrahendo Sorumluluğu*, p. 13; Eren, p. 1128; Oğuzman and Öz, Vol. I, p. 477; Hatemi and Gökyayla, p. 113.

⁴⁶⁷ Tekinay, Akman, Burcuoğlu and Altop, p. 1306; Kılıçoğlu, *Genel Hükümler*, p. 87; Gezder, *Culpa in Contrahendo*, p. 13; Nomer, p. 377.

⁴⁶⁸ Oğuzman and Öz, Vol. I, p. 477; Nomer, p. 377; Eren, p. 1156.

the actions that violate the rule of bona fides⁴⁶⁹. CIC liability arises if the parties violate these obligations by their faults during the contractual negotiations.

In Turkish law, CIC liability is not regulated by a general provision of law, this liability is mainly developed by the doctrine and judicial decisions⁴⁷⁰. However, the liabilities of the parties arising of the pre-contractual negotiations are specifically regulated by various provisions of the legislation⁴⁷¹. Three opinions dominate in the doctrine concerning CIC liability. The first one is the opinion of tort⁴⁷². According to this opinion, the parties are not tied by a contract, since they have not yet mutually and respectively expressed their wills with respect to the formation of a contract⁴⁷³. The formation of the contract and a violation of a contractual obligation are required for the application of contractual liability⁴⁷⁴. In CIC liability however, neither a contract is formed nor a contractual obligation is violated. Due to this reason, the contractual liability provisions are not applied⁴⁷⁵.

On the other hand, according to the authors defending contractual liability⁴⁷⁶ the liability to arise of the damages to occur pre-contractual negotiations is a contractual liability or quasi-contractual liability⁴⁷⁷. This is because trust relation which should not be broken is established during the contractual negotiations⁴⁷⁸ and some

⁴⁶⁹ Gezder, *Culpa in Contrahendo*, p. 182 ff.; Kılıçoğlu, *Genel Hükümler*, p. 86; Eren, p. 1157; Oğuzman and Öz, Vol. I, p. 477; It is briefly stated that the obligation to arise of the rule of bona fides in contractual negotiations is the obligation of the parties to abstain from any and all actions that would damage the counterparty. Demircioğlu, p. 122.

⁴⁷⁰ Gezder, *Culpa in Contrahendo Sorumluluğu*, p. 14.

⁴⁷¹ A party's liability, which is acting in error, for any loss or damage arising of the invalidity of the contract where the error is attributable to his/her own negligence in compliance with art. 35 of TCO, liability of the party persuading the counterparty for the conclusion of contract, for the damage to be incurred by such counterparty due to fraud and threat as stated in art. 39/f.2 of TCO or claiming the damage from the representative according to art. 47 of TCO, if such unauthorized representative performs transactions on behalf of others and such transactions are approved can be given as the examples to these provisions.

⁴⁷² For the opinions claiming that the source of this liability is tort liability, see: Gezder, *Culpa in Contrahendo*, p. 73; Oğuzman and Öz, Vol. I, p. 474; Kılıçoğlu, *Genel Hükümler*, p. 116.

⁴⁷³ Tekinay, Akman, Burcuoğlu and Altop, p. 1309.

⁴⁷⁴ Eren, p. 1158.

⁴⁷⁵ For more detailed information see: Gezder, *Culpa in Contrahendo*, p. 72-73; Eren, p. 1158.

⁴⁷⁶ For the opinions claiming that the source of CIC liability is the contractual liability, see: Gezder, *Culpa in Contrahendo*, p. 65 ff; Oğuzman and Öz, V. II, p. 475; Eren, p. 1159.

⁴⁷⁷ Eren, p. 1159.

⁴⁷⁸ Although a contractual relation is not established between the parties during contractual negotiations, a closer relation is established when compared to the third parties who have no relations with the negotiations. Due to this reason, a special kind of relation is established between the parties. See: Gezder, *Culpa in Contrahendo*, p.29.

obligations arising of the rule of bona fides are imposed on the parties during this relation⁴⁷⁹. As the parties start contractual negotiations, the obligations of performing the duty of care for each other, informing and protecting each other shall occur. Due to this reason, the provisions of contractual liability are required to be applied based on the existence of a legal relation and obligation, rather than the tort relation of the party violating these obligations by his fault⁴⁸⁰.

Based on another opinion in the doctrine, the source of CIC liability is neither tort liability nor contractual liability. According to these authors, there is a specific liability in this case⁴⁸¹. The source of this liability is based on the art. 2 of TCC. However, there are discussions among the authors claiming a special liability type, whether the liability provisions arising of tort or liability provisions arising of contractual liability shall be applied during the application of this liability⁴⁸². While some authors defend the requirement of application of contractual liability as of its consequences, other authors defend the application of the provisions of tort or contractual liabilities by taking into account the reason of the liability and the conditions of the case as per each concrete event⁴⁸³.

4.2.Culpa in Contrahendo Liability in the Protection of Personal Data

The parties negotiating in order to conclude the contract may share their personal data during such negotiations before the conclusion of the contract. However, such negotiations may not always result in the conclusion of a valid contract. In this case, many disagreements may arise with respect to the processing of personal data. These disagreements shall be solved according to the CIC liability.

⁴⁷⁹ For more detailed information see: Gezder, *Culpa in Contrahendo*, p. 74; Demircioğlu, p. 98 ff; Oğuzman and Öz, Vol. I, p. 480; Eren, p. 1131.

⁴⁸⁰ Eren, p. 1160.

⁴⁸¹ Eren, p. 1160; Demircioğlu, p. 111.

⁴⁸² The most important differences between the tort liability and the legal consequences to be caused by contractual liability are the provisions such as prescription time, proof of fault, compensation of damage and liability of the assisting person.

⁴⁸³ The authors such as *Baucher* and *Gauch/Schluep* claim opinions which are closer to contractual liability with respect to the application of the provisions. On the other hand, *Jaggi* claims that the liability provisions may vary as based on the features of the concrete case. However, he claimed an opinion which is closer to tort opinion by defending the application of prescription time of 2 years concerning the tort regulated by art. 72 of TCO with respect to prescription. Eren, pp. 1160-1161.

With the development of electronic trade, many companies started to sell over the internet. The companies selling by online marketing means without face to face conversation with the customers collect some data of the customer before the formation of a contract⁴⁸⁴. However, these companies are required to protect both the personal values and the property values of the customers during the contractual negotiations as a requirement of CIC liability. Due to this reason, unlawful processing of the personal data shall constitute an attack to the personal value of the individuals and accordingly, it is required to process in compliance with the rule of bona fides during such negotiations. Otherwise, CIC liability will occur with the formation of the other conditions.

For example, one party sends his/her name, surname and contact data to the other counterparty's database in order to conclude the contract during shopping over the internet. However, the contract is not concluded thereafter for any reason whatsoever. In this case, what will happen to the data processed or if a part of such data processed is transferred to a third party without the consent of the data subject, then the data subject's personal rights shall be damaged. The data controller's culpa in contrahendo liability arises as a result. The party whose data is processed as contrary to the good faith claims the compensation of the damage in compliance with CIC liability.

During contractual negotiations if the data of a third party are shared between the parties but somehow a contract is not formed, then CIC liability cannot be applied in this case. This is because there should be negotiations for the contract targeted to be formed in future, between the injured party and the damaging party for the application of CIC liability. Accordingly the third party whose data are processed can refer to the provisions of tort. If we are to materialize this example, a person applying to a private institution which requests reference for a training program, gives the name, surname and contact data of the reference to the private institution. However, the negotiations carried out by the parties are not concluded due to the cancellation of the training program. In case of disagreement concerning the data collected about the third parties,

⁴⁸⁴ For detailed information about the protection of the personal data, as a result of collection and use of the personal data of the individuals through various means for the purposes of online behavioral advertising, see: Berber, p. 31 ff.

the person referring with his/her capacity as a third party may demand the compensation of the damage in compliance with the provisions of tort. However, the applicant incurring damage due to such processing compensates the damage according to the provisions of CIC liability.

Moreover, some internet websites can process the data about the habits and behaviors of the users through the cookies they set in their computers. They may display the advertisements to attract the users' attention via the cookies that determine the habits and likes of them. Generally CIC liability arises in these activities which are considered as online behavioral advertising. A person's plan to shop over an internet website, entering such website and examination the features or the prices of some products or services should be considered within the frame of pre-contractual negotiations⁴⁸⁵. Meanwhile if such website processes the data through cookies, without the consent of such person, concerning the pages visited, the time spent on the mentioned pages, which products and services are examined and the frequency of such examination, then in our opinion CIC liability can be applied.

⁴⁸⁵ Entry of a consumer into the sales area or trying of the offered product or service should be considered within the scope of pre-contractual negotiation. This area is not required to be physical, any area such as advertisements, telephone internet which can influence the consumer, is appropriate for the formation of such negotiations. Gezder, *Culpa in Contrahendo*, s. 33-34.

SECTION III

ACTION FOR COMPENSATION AS A METHOD OF PROTECTION OF THE PERSONAL DATA

1. ACTION FOR COMPENSATION IN PROTECTION OF THE PERSONAL DATA

The data controller's processing of the personal data unlawfully first gives rise to tort liability. Because unlawful processing of the personal data is an activity that violates personal rights even if it is within a contractual relation. In this case, there are many protection methods which the data subject can apply to in compliance with the art. 25 of the TCC⁴⁸⁶. The data subject may file lawsuits for the protection of his/her personal rights as a result of unlawful processing of the personal data. The purpose of such lawsuits is to prevent, eliminate or terminate the effects of the attacks to the personal values⁴⁸⁷. Other than these lawsuits, if there is damage to the material or moral values because of unlawful processing of the personal data, then the data subject can file an action for compensation. Accordingly the data subject can eliminate the consequences of the attack made to the personal values and compensate his damage. Again in compliance with the same provision, if the data controller gains material income as a result of unlawful data processing activity, then the data subject can also demand the payment of such gains in compliance with the acting without authority.

When unlawful processing of the personal data is performed under a contractual relation, an action for fulfillment and avoidance of contract with compulsory execution provisions can be referred to in addition to the protection methods mentioned above⁴⁸⁸.

⁴⁸⁶ For detailed information about this, see: Oğuzman, Seliçi and Oktay-Özdemir, pp. 249-272.

⁴⁸⁷ Helvacı, *Gerçek Kişiler*, p. 159; Serozan, *Kişiler Hukuku*, p. 476.

⁴⁸⁸ Filing an action for compensation as a result of non-fulfillment of the contractual obligation does not mean the termination of the obligation relationship arising of the contract. It means that such relationship continues, however its content has changed. Eren, p. 1061; Tekinay, Akman, Burcuoğlu and Altop, p. 641.

The processing or protection of the personal data should constitute a performance obligation for the data controller in order to refer to action for fulfillment, avoidance of contract and compulsory execution provisions⁴⁸⁹. Only an action for compensation can be filed in cases where such unlawful behaviors constitute a secondary obligation.

In article 82 of the GDPR, the civil liability of the data controller or the data processor is regulated more clearly and explicitly when compared to the LPPD. Accordingly, if the data subject suffers any material or moral damage as a result of infringement of the Regulation, then he/she has the right to claim compensation of the damage suffered from the data controller or the data processor⁴⁹⁰.

The compensation receivables arise of the moment the damage occurs. However, the amount of the compensation and the form of payment is determined by the agreement of the parties⁴⁹¹ or a court decision. The compensation demand turns into a right to monetary claim together with the determination of the compensation⁴⁹². If an agreement cannot be reached about the scope of the compensation and the form of payment, the remedy which the injured party can apply to for the compensation of the damage is to file an action for compensation.

The reason of the actions for compensation is sometimes tort arising of the violation of personal rights and sometimes breach of obligations within a contractual relation. Not only moral damage but also material damage arises as a result of unlawful processing of personal data. If the action for compensation to be filed for compensating the material damage is based on tort, then provisions of art. 49 of TCO shall be applied. Contractual damages shall be subject to the provisions of art. 112 of TCO.

As a result of unlawful processing of the personal data, the data subject usually suffers moral damage. This is because the fundamental personal values such as the private

⁴⁸⁹ Eren, p. 1055.

⁴⁹⁰ Art. 82/1 of the GDPR is as; “Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.”

⁴⁹¹ Tandoğan, p. 434; This contract, is an amicable agreement concluded by and between the parties. This way, the parties conclude an agreement concerning the compensation of the damage to arise as a result of unlawful activity. Even if the amount in this agreement is more than the damage suffered, the mentioned amount cannot be contested claiming that the actual damage is different. Oğuzman and Öz, Vol. II, p. 68.

⁴⁹² Oğuzman and Öz, Vol. II, p. 68; With respect to the right to demand arising of the moral compensation being the right to claim, see: Antalya, *Manevi Zararın Belirlenmesi*, p. 47.

life, honor and dignity or self determination of the data subject are being violated with the unlawful processing of the personal data. The action for compensation shall be filed in compliance with the art. 58 of the TCO. The provision of art. 58 of TCO is applied even if the mentioned damage arises of the breach of obligation in filing an action for moral compensation. According to art. 114/2 of TCO, “*The provisions related to tort are also applied comparatively to the breach of contract*”. Accordingly, if the provisions related to the action for compensation are not specifically regulated in breach of obligation cases, then the tort provisions shall also be applied in the breach of obligations⁴⁹³.

In GDPR special emphasis is made to the moral compensation as different from the Directive no 95/46/EC. In article 23 of the Directive, it is stated that the right to demand compensation of the damage by the injured data subject as a result of processing which violates the Directive, should be provided by the Member States. However, it was not regulated whether such damage would be inclusive of the moral damages or not. As GDPR took effect, this uncertainty was eliminated⁴⁹⁴.

2. TYPES OF ACTIONS FOR COMPENSATION

2.1. Action for Material Compensation

A data subject suffering material damage as a result of unlawful processing of the personal data may claim such damages in the availability of conditions of an action for material compensation. This is because the subject of the action for compensation is constituted by the compensation of the decrease in the properties of the injured party, which occur without his/her consent, by the person (*data controller or data processor*) or persons (*joint data controllers or data controller and processor together*) responsible for the tort or action that breaches the obligation⁴⁹⁵. The subject of the material compensation within the scope of the protection of the personal data is the difference between the pre-processing and post-processing states of the properties of a person whose personal data are unlawfully processed⁴⁹⁶.

⁴⁹³ Oğuzman and Öz, Vol. II, p. 449; Baysal, p. 282; Tandoğan, p. 430; Antalya, *Manevi Zararın Belirlenmesi*, p. 37.

⁴⁹⁴ Alsenoy, p. 61.

⁴⁹⁵ Eren, p. 749; Tandoğan, p. 253; Oğuzman and Öz, Vol. II, p. 69; Korkusuz and Korkusuz, p.41.

⁴⁹⁶ Taştan, p. 175.

In cases that constitute the specific outlook forms of the personal rights and that are specifically regulated by the law, if the material compensation is specifically regulated, then such provisions are applied. An action for compensation should be filed according to the general provisions in other cases, or in cases where there is no provision for material compensation even if the personal right is regulated by a separate provision in the form of an individual outlook⁴⁹⁷.

Accordingly, although the personal data protection right is specifically regulated by the Law no 6698, the damage of the data subject shall be compensated in compliance with the general provisions since there is no special provision with respect to the compensation. This is because LPPD only refers to the general provisions concerning the form of compensation of the damages of the injured party whose personal rights are damaged due to the processing.

Finally can be stated that actions for termination of the attack, for determination of the unlawfulness and publication of such decision⁴⁹⁸, for moral compensation and for return of the gains acquired by agency without authority can be filed simultaneously with the action for material compensation arising of the processing of the personal data⁴⁹⁹. When this damage does not occur, actions for compensation cannot be opened together with the action for prevention of the attack.

In order to determine the compensation in the action for material compensation, first it is required to determine the amount of the damage. The compensation amount can never exceed the damage suffered⁵⁰⁰. The purpose of the action for damage is not to enrich the party suffering material damage due to the unlawful attack, it have such damage compensated⁵⁰¹. Due to this reason, the judge shall determine the damage first and then shall apply the required reductions by considering the provisions of the art.

⁴⁹⁷ Oğuzman, Seliçi and Oktay-Özdemir, p. 261.

⁴⁹⁸ Although the actions protecting the personal rights are lawsuits as of their nature, their remedial forms are not measurable. The claimant cannot demand the payment of a certain amount of money in these actions. Eren, p. 807.

⁴⁹⁹ Oğuzman, Seliçi and Oktay-Özdemir, p. 262; Hatemi, p. 76.

⁵⁰⁰ Mine Kaya, p. 340; Oğuzman and Öz, Vol. II, p. 114.

⁵⁰¹ Antalya, Vol. II, p. 3; Oğuzman and Öz, Vol. II, p. 114; Baysal, p. 11; Tekinay, Akman, Burcuoğlu and Altop, p. 782.

51 and 52 of the TCO and shall determine the compensation⁵⁰². Moreover, if the activity resulting in the damage brings incoincident benefits to the injured party, then such benefits are required to be reduced from the damage⁵⁰³. The burden of proof for the existence and the amount of the mentioned benefit belongs to the defendant⁵⁰⁴.

However, although extremely exceptional, in some cases there are circumstances in which the injured party is entitled to demand from the offender, compensation that exceeds the amount of the damage. The purpose of this is to have the offender abstain from acting unlawfully⁵⁰⁵. The most apparent example to this is that the person whose personal right is violated can demand the gains acquired by the offender as a result of such attack based on the provisions of agency without authority in compliance with the art. 25 of the TCC. For example, if a private hospital sells the medical data of the patients to a pharmaceutical company in consideration of money without the consent of the patients, then the data subject can demand the unlawful profit earned by the pharmaceutical company as well as the material and moral damages to be suffered.

2.1.1. Determination of the Damage

2.1.1.1. Material Damage

We stated that material damage should occur in order to file an action for material compensation. The occurrence of a material damage as a result of unlawful processing of the personal data is very rare. It is usually not possible to prove that the data subject suffered material damage due to the processing of his/her personal data⁵⁰⁶. However, there are some cases in which the data subject suffers material damage due to the unlawful processing of his/her personal data.

For example, if an insurance company collects high premiums from the data subject, who is a client, as a result of inaccurate or incomplete processing of the medical data of the data subject, then a material damage due to unlawful processing of the personal data shall occur. Again, the damages such as termination of the TV series contract of a famous actor as a result of processing of the images of a secret affair of him and

⁵⁰² Mine Kaya, p. 341.

⁵⁰³ Ayözger, p. 276; Mine Kaya, p. 341.

⁵⁰⁴ Oğuzman and Öz, Vol. II, p. 86.

⁵⁰⁵ Tekinay, Akman, Burcuoğlu and Altop, p. 786; Oğuzman and Öz, Vol. II, p. 114.

⁵⁰⁶ Çekin, *Kişisel Verilerin Korunması*, p. 102.

sharing this with the public, loss of reputation of a businessman in his community and termination of his business relations as a result of sharing data concerning his economic status and the expenses incurred in order to determine that the personal data are processed unlawfully shall constitute the material damage item.

2.1.1.2.Proof of Damage

The person to best know what types of decreases occurred in the properties or personal values of an individual as a result of tort is the injured person⁵⁰⁷. Due to this reason, the damaging party is not expected to prove the damage. The Code of Obligations takes this into account and imposes the proof of existence and amount of the damage on the injured party⁵⁰⁸. The existence and amount of the damage can be proved with any type of evidence.

In some cases however, determination of the amount or proof of the damage can be so complex that this cannot be expected from the claimant. For example, proving the amount of damage in cases of profit deprived as a result of unlawful processing of the personal data or the loss of commercial reputation sharing the personal data of a businessman via media is sometimes very difficult even impossible⁵⁰⁹. In this case, the judge determines the damage by using discretionary right. When the judge uses his discretionary right, he shall examine whether or not the unlawful processing activity is convenient for giving rise to such damage according to the ordinary course of the events and the measures taken by the injured data subject and shall determine the damage amount equitably⁵¹⁰. Judge's determination of the damage is a duty rather than an authority⁵¹¹. However, the obligation to bring the evidences that will help in determination of the damage shall belong to the claimant even in cases where the judge shall use his discretionary right in order to determine the damage⁵¹².

⁵⁰⁷ Kılıçoğlu, *Genel Hükümler*, p. 522.

⁵⁰⁸ According to art. 50/1 of TCO, "*The injured person shall be required to prove his damage and tortfeasor's fault.*"; Tandoğan, p.262; Eren, p. 749.

⁵⁰⁹ Eren, p. 750; Tandoğan, p. 263.

⁵¹⁰ Tandoğan, p. 262; Ayözger, p. 276; Eren, p. 751.

⁵¹¹ Kılıçoğlu, *Genel Hükümler*, p. 523; Supreme Court, 4. CC., D.11.12.2006, M. 2005/14955, R. 2006/13884. – Elektronik Hukuk Bankası, (Access Date: 16.03.2019).

⁵¹² Eren, p. 750.

The data subject whose personal data are unlawfully processed can also prove such damage arising of the violation of his/her personal rights, by evidences. Mainly, the damages caused by the personal data processed by using the information technologies can be determined after going through an investigation requiring technique and expertise. Due to this reason, the judge shall look in the file and shall apply to an expert in cases that require special knowledge and expertise and shall decide equitably⁵¹³.

2.1.1.3. The Date to be Taken as the Basis in the Amount of the Damage

There is no consensus in the doctrine concerning the date to be taken into account in calculation of the damage amount. This date can be the date on which the damaging event had occurred or it can be determined as the date on which the action for compensation is filed or the date on which the award is declared. The dominating opinion in the doctrine defends that the date of award should be taken as the basis in determination of the damage amount⁵¹⁴. This is because this state is clearly regulated by the art. 75 of the TCO which is related to the bodily injuries.⁵¹⁵ According to the dominating opinion in the doctrine, this rule should also be applied in the other damage cases. What is meant by the award date is the date on which the court of first instance serves or declares the decision in the action for compensation opened⁵¹⁶. It is not the date on which such decision is finalized by the Supreme Court. However, if the value of the damaged goods is decreased on the date of award, then the damage should be determined over the value on the date on which such damage had occurred or on the date on which the action is filed. This is because the compensation receivable had arisen at that time and the injured party should not suffer any more damage due to the delay in the fulfillment of the receivable⁵¹⁷.

⁵¹³ Oğuzman and Öz, Vol. II, p. 87.

⁵¹⁴ Tekinay, Akman, Burcuoğlu and Altop, p. 813; Oğuzman and Öz, Vol. II, p. 87; Eren, p. 752; Tandoğan, p. 265.

⁵¹⁵ According to the provision of the art. 75 of the TCO, “Where the consequences of the bodily injury cannot be assessed with sufficient certainty at the time of the judgment, the judge may reserve the right to amend the award within two years of the date on which the decision became definite.”

⁵¹⁶ Eren, p. 751.

⁵¹⁷ Tandoğan, p. 265.

The Supreme Court and some authors claim that the moment on which the damage had occurred should be taken as the basis⁵¹⁸. When a decision is given for the compensation receivable, delay interest shall be applied as of the date on which the damage had occurred⁵¹⁹. Despite this, if the damage cannot be remedied due to the decrease in the value, then “*compensation of the further damage which cannot be remedied by the delay interest*” can be demanded in compliance with the art. 122 of the TCO.

The opinion we share is the dominating opinion in the doctrine. The provision of the art. 75 of the TCO explicitly takes the award date as the basis. Determination of the damage amount more accurately is possible only if the award date is taken as the basis. When the judge adjudicates, he should take all the evidences, material events and relations that can be claimed until the award date into consideration⁵²⁰.

2.1.1.4. Addition of Interest to the Damage

The scope of the material damage of the data subject due to the unlawful processing of his/her personal data is inclusive of the interest receivables. The compensation receivable of the injured party arises as of the moment such damage occurs. However, the compensation of the damage shall take place by the end of the action for compensation. During this time, the person, who is deprived of the principal amount that should be paid, can also demand the interest to accrue for such period⁵²¹. If interest is demanded in the action, the amount of the damage is calculated by adding to the damage, the legal interest to accrue as of the date on which the damage had occurred. The legal interest rate is 9% according to the law.

The starting moment of the calculation of the interest is not the moment on which the tort had taken place, but the moment in which the damage had occurred. This is

⁵¹⁸ Kılıçoğlu, *Genel Hükümler*, p. 525.

⁵¹⁹ Kılıçoğlu, *Genel Hükümler*, p. 525.

⁵²⁰ Eren, p. 752. According to Tekinay, calculation of the damage based on the economic value which may belong to years before, can cause the compensation to be awarded to be insufficient. Due to this reason, the damage should be calculated as based on the date of the award. However, if the value of the goods was raised in between and reduced on the date of award, then the damaged goods should be calculated as based on the highest value reached. Tekinay, Akman, Burcuoğlu and Altop, p. 813.

⁵²¹ Eren, p. 753.

because the damage can sometimes occur much later than the moment on which the tort had occurred. The interest can be applied only in cases where there is damage⁵²². The judge accrues the legal interest from the moment in which the damage had occurred until the moment in which the decision is given. After awarding the compensation, default interest accrues for the unpaid compensation⁵²³.

2.1.1.5. Balancing

The data subject may sometimes acquire economic benefits in addition to the damages suffered as a result of unlawful processing of the personal data. How shall these benefits influence the calculation of the material damage? The general rule is that if a benefit is acquired as a result of the damaging behavior, then such economic benefit should be reduced from the damage⁵²⁴. Otherwise, the injured party shall acquire unjust enrichment⁵²⁵. The purpose of the liability law is not to enrich the injured party but to remedy such damage by payment of compensation⁵²⁶.

In order to apply the balancing rule, there should be a damage requiring compensation, a benefit to be balanced with the damage and an appropriate causal relationship between the activity resulting in damage and the benefit⁵²⁷. In other words, an appropriate causal relationship should exist between the damaging activity and the benefit. If the benefit to occur is a coincidental and extraordinary consequence created by the tort, rather than being the ordinary consequence of the tort, then balancing cannot be applied. For example, a private hospital leaked the sexual preferences of a famous actor to the media. As a result of this, the advertising and movie contracts of the actor, who received considerable reactions from the community, are terminated. However, after some time, a director in America offered to this actor who was on the

⁵²² Eren, p. 753.

⁵²³ Eren, p. 754.

⁵²⁴ Tandoğan, p. 267; Eren, p. 754; This condition is also included in the Supreme Court decisions. The Supreme Court 4 CC.'s decision dated 23.05.1978 “... since the purpose of the compensation is to remedy the decrease in the properties and to provide the previous state of the properties, netting of the damage by reduction of the benefits provided to the injured party as a result of the damaging event are, from the damage amount is a requirement and consequence of the general compensation provisions...” Supreme Court, 4.CC., D. 23.05.1978, M. 1978/5699, R. 1978/6860 – Legalbank Elektronik Hukuk Bankası, (Access Date: 16.02.2019)

⁵²⁵ Tekinay, Akman, Burcuoğlu and Altop, p. 789.

⁵²⁶ Antalya, Vol. II, p. 4; Tandoğan, p.267.

⁵²⁷ Tekinay, Akman, Burcuoğlu and Altop, p. 791.

agenda as a result of such reactions, a role to play a gay character in the movie. In this case, the actor, whose advertising and movie contracts were terminated due to the leakage of the personal data to the media, did not suffer any material damage. However, he became more famous and signed another contract for a movie in America. Accordingly, the judge shall not apply any balancing for the material compensation. This is because although the mentioned benefit is a result of a tort, it cannot be considered as an ordinary consequence of the tort in the ordinary course of life.

Balancing rule can be applied in tort liability and also in the liability to arise of contractual relation. However, balancing cannot be applied in cases where there are moral damages⁵²⁸. Due to this reason, such benefits do not influence the compensation of the moral damage suffered even if the data subject have acquired a material benefit as a result of leakage of his/her personal data. For example, in the example given above, even if the actor whose personal data are leaked, acquires an economic benefit due to such leakage, this shall not influence the moral damage which occurred. This state shall not constitute a reason for reduction in the moral damage.

If the judge concludes from the file that the injured party acquires a material benefit due to the damaging activity, then he/she applies the balancing rule ex officio during the calculation of the damage amount. However, as a rule, the burden of proof for the existence and amount of the benefit acquired by the data subject shall belong to the data controller who is in the position of the damaging party⁵²⁹. In cases where the accurate amount of the mentioned benefit cannot be calculated, the judge determines it based on his/her discretionary power according to the art. 50/II of the TCO.

2.1.2. Determination of the Compensation

The purpose for filing an action as a result of tort or breach of obligation is to remedy the damage. On the other hand, the purpose of the material compensation is to provide the property of the injured party to be in the state in which such property would be if the damaging event had not occurred⁵³⁰. Due to this reason, the damage constitutes the upper limit of the compensation to be awarded⁵³¹. The judge primarily shall determine

⁵²⁸ Eren, p.756.

⁵²⁹ Tandoğan, p. 273; Eren, p. 756.

⁵³⁰ Eren, p. 787.

⁵³¹ Tekinay, Akman, Burcuoğlu and Altop, p. 785; Kılıçoğlu, *Genel Hükümler*, p. 533; Eren, p. 787.

the damage and shall determine the compensation to be decided over the damage that had occurred. After determination of the damage, the judge may apply reductions in the compensation amount as based on some reasons. In this case, the compensation amount calculated would be below the damage⁵³².

In Turkish Code of Obligations, the judge is given the power to determine the scope of the compensation and the form of payment. Accordingly, the judge shall determine the amount and form of payment of the compensation according to the nature of the case in question. During this time, it is also required to take into account, the severity of the damaging party's fault. The judge can also decide the payment of the compensation in the form of annuity. However, a guarantee concerning the payment of the debt in future is demanded from the debtor when deciding for such annuity.

2.1.2.1. Factors Effecting the Material Compensation

The judge shall determine the compensation amount by taking various factors into consideration. This is expressed as "*The judge determines the extent and the form of the compensation with due regard to the circumstances and particularly the degree of culpability*" in the art. 51/1 of the TCO.

It is required to examine the nature of the case in question when determining the amount of the compensation. In the case in question, the form of the performance of the unlawful behavior shall specifically be significant⁵³³. During the unlawful processing of the personal data, the differences in the nature of the activity when a person uses special technical means and processes the personal data, or when a person processes manually without automatic means may affect the calculation of the compensation amount. Or since the risk to be subject to discrimination by some communities due to the unlawful processing of the personal data of special nature, which is a type of personal data, it shall be taken into consideration calculation of the compensation⁵³⁴.

In fault liability, the degree of the fault of the damaging party is not important for the compensation of the damage of the injured party as a rule. The damaging, either with

⁵³² Tandoğan, p. 315.

⁵³³ Kılıçoğlu, *Genel Hükümler*, p. 534.

⁵³⁴ Ayözger, p. 276.

slight or severe fault, is required to compensate the damage of the injured party. With respect to the liability due to the breach of obligation, it is clearly stated in the art. 114/I of the TCO that the debtor shall be liable for any and all faults in general.

However, in some cases, specifically in the cases where the damaging party has a slight fault, the judge may be required to make reduction in the compensation as a requirement of the feelings of justice and equity⁵³⁵. Consequently, the art. 51/1 of the TCO requires the judge to take the degree of the damaging party's fault into consideration, when determining the extent and form of payment of the compensation. And again, in the art. 52/2 of the TCO, it is stated that if equitable considerations require it, the judge may reduce the compensation award in cases in which the payment of such compensation by the liable person, who has caused the damage by slight negligence, would leave him in financial hardship. Accordingly, if the data controller has gross fault in unlawful processing of the personal data, then the damage amount and the compensation amount can be equal. However, in cases where the data controller has a slight fault, the judge may decide the compensation to be less than the damage that had occurred. In this case, the law provided the discretionary right to the judge⁵³⁶. If there is a slight fault, the judge is not required to make a reduction in the compensation⁵³⁷.

However, when the data controller has strict liability, the fault shall not be taken into consideration and having a slight or no-fault shall not constitute a reason of reduction in the compensation. For example, if the data controller, as the employer, is in the position of defendant, the judge shall not take this into consideration for the unlawful processing of personal data performed by his/her employee, even if there is slight fault or no-fault. In the action failed by the data subject directly against the employee, the slight fault can be a reason for reduction in the compensation⁵³⁸.

⁵³⁵ Tandoğan, p. 317; Eren, p. 789.

⁵³⁶ Tekinay, Akman, Burcuoğlu and Altop, p. 797; Ayözger, p. 277.

⁵³⁷ Eren, p. 789; The judge may take the nature of the event, financial states of the parties and their relations with each other and may decide not to make a reduction. Tekinay, Akman, Burcuoğlu and Altop, p. 797.

⁵³⁸ Ayözger, p. 278.

2.1.2.2.Reduction Reasons in the Material Compensation

The art. 52 of the TCO regulates the reasons of reduction in calculation of the compensation. This is mainly related to the effect of the activities of the injured party, on the compensation⁵³⁹. The injured party's consent to the damaging activity and common fault is a clear indication of this state⁵⁴⁰. The reduction reasons for the compensation are applied in the liability due to the breach of obligation, unless there is a contrary provision.

Accordingly, the injured party's consent for the damaging activity shall be considered as a reduction reason for the compensation. However, it should be stated that the explicit consent regulated by the LPPD and the consent regulated by the art. 24/2 of TCC is different in function from the consent regulated by the mentioned provision. The explicit consent mentioned in the LPPD and the consent concept regulated by the art. 24/2 of the TCC are the reasons of lawfulness⁵⁴¹. In these cases, breach of obligation or tort liability is not the issue. Accordingly, no compensation can be decided.

However, what is meant by the consent regulated by the art. 52 of the TCO is the consent given unlawfully or non-ethically⁵⁴². Accordingly, the consent given unlawfully or non-ethically shall be accepted as invalid according to the art. 23 of the TCC. For example, the processing activity that is contrary to the general principles concerning the processing of the personal data stated in the art. 4 of the LPPD shall be accepted as unlawful even if the data subject consents such processing. And accordingly, the private law liability of the data controller arises. However, the judge may accept this consent of the injured data subject as a reason for reduction in the compensation or for refusal of the compensation demand⁵⁴³. This is because the

⁵³⁹ Eren, p. 788; the art. 52/1 of the TCO appears as a special outlook of the rule of bona fides in liability law. An individual's demand for compensation for the damages which he/she could have prevented is contrary to the rule of bona fides. Baysal, p. 29.

⁵⁴⁰ For detailed information about the injured party's fault and the effect of the fault on the compensation, see: Başak Baysal, *Zarar Görenin Kusuru-(Müterafik Kusur)*, İstanbul: Onikilevha Yayıncılık.

⁵⁴¹ Hatemi, p. 69; Baysal, p. 44.

⁵⁴² Tekinay, Akman, Burcuoğlu and Altop, p. 661; Eren, p. 790; Baysal, p. 44.

⁵⁴³ Kılıçoğlu, *Genel Hükümler*, p. 526; Tekinay, Akman, Burcuoğlu and Altop, p. 662.

consent given by the data controller is a different outlook of the common fault⁵⁴⁴. Le Due to this reason, payment of all the compensation may not be equitable.

If the injured data subject is faulty for the occurrence or increase of the mentioned damage, then the judge may choose to apply reduction in the compensation.

The art. 52 of the TCO states that “*where the injured person consented to the action which caused the damage or helped give rise to or compound the damage or otherwise exacerbated the position of the person liable for it,*” the judge may reduce the compensation due or even dispense with it entirely. The injured party’s fault mentioned here is not in the nature of gross fault⁵⁴⁵. This is because the injured party’s gross fault shall break the causal relationship and then no compensation liability shall arise⁵⁴⁶. An example to this is the drawing of a person’s deposit in a bank as a result of the data subject’s sharing of such bank data with a third party by his/her own gross fault.

However, if the data subject’s fault is not in the nature of gross fault, then the compensation liability of the data controller acting in breach of the obligation or the general codes of conduct shall continue. In this case, the judge shall decide to reduce or reject the compensation demand by taking the fault of the injured data subject into consideration⁵⁴⁷. An example to this is when the subscriber of a telecommunication company registers his/her contact data by mistake in the subscribers’ guide, which can easily be accessed by everyone⁵⁴⁸. In this case if the enterprise did not take the required measures and perform the consent procedures, then it shall be liable for the processing of the personal data. However, reduction may be applied in the compensation since there is common fault.

⁵⁴⁴ Eren, p.7 90.

⁵⁴⁵ Tandoğan, p.319.

⁵⁴⁶ Tandoğan, p.318; Kılıçoğlu, *Genel Hükümler*, p. 537; Eren, p.791.

⁵⁴⁷ Eren, p. 792; Tekinay, Akman, Burcuoğlu and Altop, p. 805; The judge is required to take the injured party’s fault into consideration ex officio when determining the compensation amount. Baysal, p. 30; Attention is drawn to this issue in the Supreme Court Assembly of Civil Chamber decisions. Supreme Court, ACC., D.12.06.1997, E. 1996/ 11-372, R. 1996/ 485.- Elektronik Hukuk Bilgi Bankası, (Access Date: 20.02.2019)

⁵⁴⁸ Ayözger, p. 279.

The data subject should take any and all measures in order to prevent the increase in the damage that occurs as a result of unlawful acquisition of the personal data. For example, a person noticing that money is drawn from his/her account without his/her consent should promptly notify the relevant bank about this and demand the stop of the account flow. If a person thinking that money is drawn from his/her account delays in notifying this to the bank and causes more money to be drawn from the account in future, then the judge should take the data subject's fault into consideration during determination of the compensation amount⁵⁴⁹. The burden of not increasing the damage is not a duty which is only imposed on the injured party. The damaging party also makes efforts in order not to increase the damage in compliance with the rule of bona fides⁵⁵⁰. Due to this reason, as the data controller becomes aware that the personal data are unlawfully processed or acquired, he/she should notify the data subject and the Personal Data Protection Authority in soonest time possible.

The fault and common fault of the data controller and the data subject in the damages to occur as a result of processing of the personal data are generally determined by the experts. This is because it requires expertise to determine the faults of the data controllers, who use some technical means by benefitting from various facilities of the technology, in unlawful processing of the personal data. In this case, the judge shall send the file to an expert and shall decide about the compensation as based on the expertise report.

2.1.3. The Relation between the Action for Material Compensation and the Action for Agency Without Authority

The individuals whose personal rights are violated can demand the gains acquired by the offender as a result of such violation according to the provisions of agency without

⁵⁴⁹ As it is known, the injured party's fault occurs in two ways in the application. The first one is the direct participation of the injured party in the occurrence of the damage (common fault) and the second one is causing an increase in the damage which occurred (the burden of mitigating, not increasing the damage). The second one applies to this case. This condition is laid as a burden on the data subject. A burden is imposed on the data subject who is the injured party, for not acting in a manner to cause the occurrence and increase of the damage. Burden can be defined as the obligations which would result in the total or partial loss of the rights of a person who does not fulfill some behavioral duties imposed on him/her. Baysal, p. 30.

⁵⁵⁰ Baysal, p. 50.

authority in the art. 25/3 of the TCC. In other words, the person whose personal rights are attacked as a result of unlawful processing of the personal data can demand the gains earned by the offender as a result of such unlawful activity in compliance with the provisions of false agency without authority in the art. 530 of TCO.

In false agency without authority, there is the will to acquire gains for his/her own benefit rather than the benefit of the owner of the work⁵⁵¹. In an action for false agency without authority, a gain which the injured party does not desire to or cannot acquire is acquired by the offender as an unlawful attack⁵⁵². However, in an action for material compensation, the offender destroys a gain, which the injured party desires to acquire or can acquire, as a result of the unlawful attack and in other words, causes a decrease in the properties of the injured party. For example, in cases where a person is caused to draw a credit from a bank with a high rate of interest as a result of faulty processing of his/her data concerning his/her economic status, then such person remedies the material damage suffered, by an action for compensation to be filed. However, if an employee working in the land registry office sells the identity data of the owners of the properties in an area where expropriation is applied, to a law office in consideration of money, then the data subjects can demand this gain as based on the provisions of false agency without authority.

There is a dispute in the doctrine whether or not an action for material compensation and provisions of false agency without authority can be applied simultaneously⁵⁵³. According to one opinion, the claimant shall either file an action for material compensation due to the damage suffered or shall demand the gain acquired by the offender⁵⁵⁴. According to another opinion, these two actions can be filed simultaneously under some circumstances⁵⁵⁵. In our opinion, the data subject should be able to file both the action for material compensation and for agency without authority simultaneously against the data controller. While the purpose of the material compensation is to remedy the damage suffered by the data subject, the purpose of the action for false agency without authority is to provide that the gains acquired by the

⁵⁵¹ Hatemi, *Kişiler*, p. 78.

⁵⁵² Ümit Gezder, *Türk Medeni Hukuku-(Başlangıç-Kişiler-Aile Hukuku)*, (İstanbul: Beta, 2014), p. 43.

⁵⁵³ Gezder, *Türk Medeni Hukuku*, p. 43; Hatemi, p. 78-79.

⁵⁵⁴ Hatemi, p. 79.

⁵⁵⁵ Dural and Ögüz, p. 158; Oğuzman, Seliçi and Oktay-Özdemir, p. 270.

offender as a result of an unlawful activity do not remain with him/her. However, if a part of the gains acquired as a result of agency without authority covers the damage of the data subject, then only the gains due to agency without authority should be demanded.

2.2.Action for Moral Compensation

Action for moral compensation aims to remedy the pain, suffering and sorrow of the injured party as a result of the attack on his/her personal rights⁵⁵⁶. The moral compensation was subject to strict and up to date regulations in the recent periods in order to better protect the personal rights and values of the individuals. The most important reasons for this are the rapid development in the information and communication technologies sector, more complex social relations and the risk of easier violation of the personal values of the individuals. Unlawful processing of the personal data is considered as an attack to a person's personality rights such as private life, human dignity, honor and reputation and his/her right to determine his/her own destiny. In this case, the data subject shall be subject to moral damage and an action for moral compensation can be filed in order to remedy such damage⁵⁵⁷.

The remedy provided for the elimination of the damage that occurred is to pay some amount of money to the injured party⁵⁵⁸. In an action for moral compensation the claimant party shall demand some amount of money for the mitigation of the pain, sorrow and suffering incurred. The art. 58 of the TCO gives discretionary authority to

⁵⁵⁶ Oğuzman, Seliçi and Oktay-Özdemir, p. 263; Tandoğan, p. 330; There are various opinions in the doctrine with respect to the purpose of the moral compensation. Those claiming that the purpose of the moral compensation is to punish the offender take the offender's fault as the basis. According to them, the moral compensation has a punishing and preventive function. A generally accepted opinion in the doctrine, considers the moral compensation as an instrument to mitigate the pain suffered by the injured party. This opinion which is accepted as satisfaction opinion is close to subjective moral damage theory. According to another opinion, the purpose of the moral compensation is to compensate the moral damage incurred, in kind or as cash. For detailed information, see: Kılıçoğlu, *Genel Hükümler*, p. 553; Eren, pp. 809-812.

⁵⁵⁷ Supreme Court, ACC., D.17.06.2015, M. 2014/56, R. 2015/1679. - Legalbank Elektronik Hukuk Bankası (Access Date: 10.01.2019); Supreme Court, 4CC., D. 13.12.2017, M. 2016/2970, R. 2017/8273. - Legalbank Elektronik Hukuk Bankası (Access Date: 20.03.2019).

⁵⁵⁸ Cannot be considered as an actual damage-compensation action cannot be considered. It is more in the nature of relieving the counterparty's pain and deterrent punishment. Serozan, *Kişiler Hukuku*, p. 477; Tekinay, Akman, Burcuoğlu and Altop, p. 877; Korkusuz and Korkusuz, p. 42; Antalya, *Manevi Zararın Belirlenmesi*, p. 8; Arıdemir, p. 12.

the judge in order to remedy such damage. According to this provision, the judge may decide the compensation of this damage not by money but by any other form of elimination or by an additional elimination together with certain amount of compensation. Or, the judge may give a decision condemning the abuse and decide the publication of this decision.

There are special provisions⁵⁵⁹ in the TCC and TCO arranging the moral compensation as a result of violation of some personal values. Other than these, in case of violation of the other personal right values, the provision of the art. 58 of TCO contains a general provision for the moral compensation⁵⁶⁰. In case of violation of all other personal values which are not regulated specifically in the TCC and TCO, the injured party may file an action for the moral compensation according to this provision. The person suffering moral damage as a result of unlawful processing of the personal data can demand moral compensation according to art. 14/ğ of the LPPD and the art.5 8 of TCO and art. 25 of TCC.

The activity causing damages in the personal values of the individual may arise of tort as well as breach of obligation. In this case, although the provisions of the moral compensation are regulated within the provisions concerning tort, it shall also be applied to the breach of obligation comparatively in compliance with the art. 114/2 of TCO⁵⁶¹. For claiming moral compensation in the event of breach of obligation, violation of the counterparty's personal rights and occurrence of a moral damage as a result of this are sought⁵⁶².

The unlawful activity is not required to be directly directed to the personal values. In some cases, a person may suffer moral damage as a result of an attack to the property and an action for compensation can be filed as a result⁵⁶³. In an action for moral compensation, two stages, as to determine the damage and then to determine the

⁵⁵⁹ The provisions such as the usurpation of name (art. 26/2 of TCC); disengagement (art. 121 of TCC), death and bodily injury (art. 56 of TCO) specifically regulate the moral compensation.

⁵⁶⁰ Antalya, *Manevi Zararın Belirlenmesi*, p. 11.

⁵⁶¹ Eren, p. 806; Antalya, *Manevi Zararın Belirlenmesi*, p. 13; Arıdemir, p. 47 ff.

⁵⁶² Oğuzman, Seliçi and Oktay-Özdemir, p. 268.

⁵⁶³ Kılıçoğlu, *Genel Hükümler*, p. 553.

amount of the compensation like in an action for material compensation, are not required⁵⁶⁴.

2.2.1. Theories Explaining Moral Damage Concept

In order award moral compensation, all the conditions of the liability law are required to be realized. However, the factor of damage to occur here should occur in the moral world of the person⁵⁶⁵. The subject of discussion in this issue is whether or not an attack made to the personal values of an individual is sufficient for the formation of moral damage⁵⁶⁶. According to the objective opinion, the objective reduction in the personal values of an individual as a result of an attack made only to the personal values shall constitute the moral damage⁵⁶⁷. According to this opinion, the moral damage occurs as independent of the person whose personal rights are attacked. An attack to the personal values is sufficient for the occurrence of a moral damage, and it is not required to have any emotional, psychological or physical damage on the person whose personal right is attacked, due to such violation⁵⁶⁸. For example, unlawful processing of the personal data or transfer of them to the third parties constitutes an attack to the personal values on its own. Even if the data subject suffers any moral and psychological damage due to this processing, he/she can demand moral compensation

⁵⁶⁴ Oğuzman, Seliçi and Oktay-Özdemir, p. 266; The compensation of the moral loss and the compensation of the material damage are calculated separately even for the same event. This is because the legal facts of the material compensation and the legal facts of the moral compensation are different. Due to this reason, the judge cannot consider the material and moral compensation together and determine a joint compensation amount. Antalya, *Manevi Zararın Belirlenmesi*, p. 9.

⁵⁶⁵ Tekinay divides the moral damages requiring the payment of compensation into three categories. These are: 1) Pain and sorrow due to the violation of bodily integrity; 2) Pain and sorrow in case of death felt by the individuals who are closely related to the deceases person and finally 3) Pain and sorrow arising of the violation of the personal rights. Tekinay, Akman, Burcuoğlu and Altop, p. 878.

⁵⁶⁶ For these discussions, see: Antalya, *Manevi Zararın Belirlenmesi*, p. 13; Hülya Atlan, *Manevi Zararı Tazmin Yolları* (İstanbul: Onikilevha Yayıncılık, 2015), p. 47.

⁵⁶⁷ Antalya, *Manevi Zararın Belirlenmesi*, p. 17; Atlan, p. 50; Supreme Court, accepts the objective theory in some of the decisions. According to the Supreme Court 4.CC's decision, "Moral damage is an objective reduction in the personal values. Pain felt, suffering incurred may occur not as a moral damage but an outlook of such moral damage. Qualification of the pain and sorrow as moral damage restricts the legal persons and those who are unconscious; and on the other hand, laws restrict the facts for which moral compensation can be given in order not to deprive those, who hide their pains in themselves, of their rights to demand compensation. These are damaging of the personal rights as a result of one of the following cases: damage to the personal values (art. 24 of TCC), attack to name (art. 26 of TCC), disengagement (art. 121 of TCC), termination of marriage (art.158 of TCC), causing bodily injury or death (art. 47 of TCO)" Supreme Court, 4.CC., D.15.03.2016, M. 2015/16627, R. 2016/3407- Legalbank Elektronik Hukuk Bankası, (Access Date: 28.04.2019).

⁵⁶⁸ Atlan, p. 51; Aridemir, p. 8.

since the attack to the personal values had occurred. This opinion was criticized for not considering the emotional damages with respect to the pain, sorrow and suffering felt by the individual as a result of violation of his/her personal values⁵⁶⁹. This state shall cause the payment of the same compensation amount to the persons who are affected differently from the attack, which will be contrary to the remedy purpose of the compensation.

According to the subjective opinion, occurrence of an attack only to the personal values is not sufficient for the formation of the moral damage, it is also required that the person being attacked feels pain, sorrow and suffering⁵⁷⁰. For the formation of moral damage, the person, whose personal right is violated, should be affected morally and psychologically or there should be a decrease in his/her joy of living⁵⁷¹. In other words, damage should occur in the emotional world of the individual⁵⁷². This theory is criticized because those lacking the power of discernment or those legal persons shall be deprived of the moral compensation demand since they shall not be influenced psychologically and morally when an attack is made to their personal values⁵⁷³. And again this is criticized because of the impossibility to accurately and definitely determine the pain and sorrow felt by each individual for the violation of his/her personal rights, different levels of influence on each individual for the pain and sorrow felt for the same attack, which will make it difficult to determine the moral damage⁵⁷⁴. The reaction of the person whose personal rights are attacked may vary as based on the social life, character, personality, education and social status of such person⁵⁷⁵.

⁵⁶⁹ Antalya, *Manevi Zararın Belirlenmesi*, p. 17.

⁵⁷⁰ This opinion is the opinion that is generally accepted in the doctrine. Kemal Tahir Gürsoy, "Manevi Zarar ve Tazmini", *AÜHFD*, V. XXX, Issue. 1 (1973), p. 1-4, p. 8; Antalya, *Manevi Zararın Belirlenmesi*, p. 14; Tekinay, Akman, Burcuoğlu and Altop, p. 655; Oğuzman, Seliçi and Oktay-Özdemir, p. 263-265; Dural and Ögüz, p. 160; Reisoğlu, p. 204; Helvacı, *Kişilik Hakkı*, p. 177.

⁵⁷¹ Arıdemir, p. 14; In most decisions of the Supreme Court, we see that the subjective opinion is acquired. Supreme Court, 3.CC., D.24.02.2014, M. 2013/18799, R. 2014/2717- Legalbank Elektronik Bilgi Havuzu (Access Date, 10.03.2019).

⁵⁷² Oğuzman and Öz, Vol. II, p. 39; Dural and Ögüz, p. 160; Atlan, p. 48; Antalya, *Manevi Zararın Hesaplanması*, p. 15.

⁵⁷³ Eren, p. 484; Rona Serozan, "Manevi Tazminat İstemine Değişik Bir Yaklaşım", Tribute to Prof. Dr. Haluk Tandoğan, *Banka ve Ticaret Hukuku Araştırmaları Dergisi* (Ankara, 1990), p. 82.

⁵⁷⁴ Atlan, p. 50; Antalya, *Manevi Zararın Hesaplanması*, p. 95; Arıdemir, p. 180.

⁵⁷⁵ Arıdemir, p. 179; Serozan, *Manevi Tazminat İstemine Değişik Bir Yaklaşım*, p. 82.

⁵⁷⁶ Atlan, p. 50; Antalya, *Manevi Zararın Hesaplanması*, p. 16

Another opinion concerning the moral damage is the *mixed opinion*. According to this opinion, the objective reduction as a result of the attack made to the personal values and the reduction created in the moral and psychological world of the individual caused by the pain, sorrow and suffering felt by the injured party as a result of this attack should be considered together⁵⁷⁶. According to *Antalya*, the objective factor defended by the objective theory should be completed with the subjective factor defended by the subjective theory and accordingly, the moral damage should be formed of these two factors⁵⁷⁷. Moral damage is the pain suffered by the injured party as a result of the objective reduction taking place in the personality⁵⁷⁸. According to the author, the attack qualified for the formation of the moral damage should influence the individual psychologically and morally in the inside and also his/her economic and social life on the outside. Based on this opinion, for a person to suffer moral damage, there should be a reduction as a result of an attack to the personal values and such reduction should cause a reduction in such person's joy of living, destruction of his/her moral and psychological balance, and feelings of pain or sorrow⁵⁷⁹.

In our opinion, violation of the personal values should be considered as a compulsory factor for the formation of the objective factor of the moral damage and this factor should be sought in all cases. However, apart from the objective theory, the developments in the inner world of the individual such as the extent of the influence of the violation on the moral and emotional world of the individual, the intensity of the pain, grief and sorrow felt should also be effective for determination of the moral damage. Accordingly, the destruction of the moral and psychological integrity of the individuals as a result of the attack on the personal values, depression or feelings of pain and sorrow shall be influential on the determination of the compensation and be appropriate for the remedy purpose of the action for compensation.

⁵⁷⁶ This theory was first claim by *Tercier. Pierre Tercier, Contribution a l'etude du tort moral et de sa reparation en droit civil suisse*, These, Fribourg, 1971. Quoted by; Aridemir, p. 181; *Antalya, Manevi Zararin Belirlenmesi*, p. 18.

⁵⁷⁷ *Antalya, Manevi Zararin Belirlenmesi*, p. 19.

⁵⁷⁸ Necip Kocayusufpaşaoğlu, "Kişilik Haklarını Koruyan Manevi Tazminat Davasına İlişkin Yeni Gelişmeler", Sorumluluk Hukukunda Yeni Gelişmeler I. Sempozyumu, Ankara, 21-22 Ekim 1977, İstanbul, Fakülteler Matbaası, 1980, p. 147; Aridemir, p. 182.

⁵⁷⁹ *Atlan*, p. 53; Aridemir, p. 182.

2.2.2. Moral Damage on the Basis of the Personal Data

The processing activities such as unlawful registration, storage, use of the personal data or sharing such data with a third party constitute a direct attack to the personal area of the data subject. For example, if a telephone call between two people is wiretapped and recorded⁵⁸⁰, this shall constitute a direct intervention of such person's privacy, freedom of communication and the right to determine his/her own destiny. In cases accepted by the objective theory, moral damage shall occur when processing activities such as unlawful acquisition, use, transfer of the personal data are performed and the data subject can demand moral compensation due to the attack performed to their personalities. According to a decision of the Supreme Court dated 2017⁵⁸¹, access of a person's personal data in an unlawful manner is sufficient for the occurrence of the moral damage. According to this decision, *"The defendant declared during the penal judgment that he took the claimant's "e-state" password and accessed the personal data of the claimant, together with his daughters. The claimant's moral damage occurred since this is also accepted by the court. It is not correct to dismiss the case wherein it is required to decide some amount of moral compensation appropriate for the benefit of the claimant."* and the award was made as based on the objective theory.

As expressed above, unlawful attack to the personality shall not be enough for the formation of the moral damage in cases where the subjective theory or the mixed theory is adopted, it is also required that there should be moral and psychological effect on the data subject. Accordingly, demand for moral compensation cannot be made since unlawful processing of the personal data only shall not be sufficient for the formation of the moral damage. For example, moral damage is not formed in case the processing of the data of a student whose medical data were unlawfully processed by the university personnel, does not have any psychological and moral effect on the person. However, the emotional trauma suffered by the student who is very sorry and whose relations with his friends are destroyed as a result of sending such medical data processed by e-mail to the student's friends by mistake constitutes moral damage. In

⁵⁸⁰ Ayözger, p. 280.

⁵⁸¹ Supreme Court, 4CC., D.13.12.2017, M. 2016/2970, R. 2017/8273. - Legalbank Elektronik Hukuk Bankası (Access Date: 20.03.2019).

our opinion, processing of the personal data only shall not be sufficient for the formation of moral damage in compliance with the mixed opinion. As a result of this processing, there shall be negative results on the data subject psychologically and morally. However, only the reduction on the personal values may form the moral damage for the protection of the person without power of discernment or the legal person.

2.2.3. Determination of the Moral Compensation

Since the reduction of the personal values cannot be calculated as an economic value and since the compensation cannot be determined accordingly, a broad discretionary power is given to the judge in the actions for moral compensation⁵⁸². Despite this discretionary power, the judge is bound by the demand of the claimant in determination of the moral damage⁵⁸³. Due to this reason, even if it is required to give compensation more than the amount demanded by the claimant based on the conditions, the judge cannot decide the payment of an amount which is more than the amount demanded by the claimant⁵⁸⁴. However, the judge can decide the payment of an amount that is less than the demanded amount as based on the conditions. In other words, the judge uses the discretionary power in a manner not to exceed the amount demanded by the injured party. What is important here is to avoid determination of a lower amount which does not satisfy the injured party and which does not serve justice. Likewise, the decision for the payment of a higher amount, which would be like an award for the injured party, should also be avoided⁵⁸⁵.

⁵⁸² Since determination of a net monetary value for the moral damage is impossible, it is not possible to compensate the damage in full. Antalya, *Manevi Zararın Belirlenmesi*, p. 9; Eren, p. 821; Atlan, p. 81; Arıdemir, p. 70.

⁵⁸³ Since the damage cannot be determined in full, the stage of calculation of the damage in the action for material compensation does not exist in the action for moral compensation. Here the judge determines the compensation in compliance with the law and equity according to the art. 4 of the TCC. Antalya, *Manevi Zararın Hesaplanması*, p. 75; Arıdemir, p. 70.

⁵⁸⁴ Oğuzman, Seliçi and Oktay-Özdemir, p. 265; even if the material compensation can be determined as foreign currency, the moral compensation should only be determined as Turkish Lira. Antalya, *Manevi Zararın Hesaplanması*, p. 74.

⁵⁸⁵ Oğuzman, Seliçi and Oktay-Özdemir, p. 265.

When determining the moral compensation, the judge should also apply the provisions of the art. 51 and 52 of the TCC comparatively⁵⁸⁶. Due to this reason, when determining the amount of the moral compensation for the violation of the personal right as a result of unlawful processing of the personal data, the judge takes the scope and amount of the processing activity of the data controller, whether these are processed automatically or non-automatically, the data controller's or the processor's ratio of fault, the social and economic states of the parties into consideration⁵⁸⁷. Moreover, again according to these provisions, the degree of the damaging party's fault, conditions of common fault or the consent of the data subject can cause reduction in the compensation. It should be expressed here that while the severity of the damage is influential on the determination of the moral damage, the fault of the data controller plays a significant role in calculation of the moral compensation⁵⁸⁸. On the other hand, if the fault of the data subject is at a level to break the causal relationship, then the data controller is relieved of the liability⁵⁸⁹.

In addition, the damaging party being driven into poverty when the compensation is paid in full, the injured party's economic status being very well, the effect of an unexpected event in the occurrence of the damage and the personal relations between the injured party and the damaging party, can all be effective in determination of the compensation⁵⁹⁰.

3. PARTIES OF THE ACTION FOR COMPENSATION

3.1.Claimant

3.1.1. Data Subject

The data subject whose personal rights are attacked or have been attacked as a result of the unlawful processing of the personal data shall have the capacity of a claimant in

⁵⁸⁶ Eren, p. 820; Antalya, *Manevi Zararın Belirlenmesi*, p. 73.

⁵⁸⁷ Supreme Court, 4CC., D.18.12.2013, M. 2013/2039, R. 2013/20094. – Legalbank Elektronik Hukuk Bankası, (Access Date: 16.03.2019); Ayözger, p. 283; Antalya, *Manevi Zararın Belirlenmesi*, p. 58; Arıdemir, p. 72.

⁵⁸⁸ Antalya, *Manevi Zararın Belirlenmesi*, p. 58.

⁵⁸⁹ Eren, p. 820.

⁵⁹⁰ Eren, p. 821.

the action for compensation to be filed⁵⁹¹. As a rule, only the individuals who are directly damaged have the right to file action for compensation⁵⁹². Other than this, the individuals suffering damage by reflection can file an action only if there is a relation of unlawfulness⁵⁹³. For example, if the personal data of a singer, related to the singer's conviction of infamous crime committed before, is leaked to the media, the concerts may be cancelled due to the public's reaction. In this case, the singer shall suffer a direct damage due to such leakage and shall be able to file an action for compensation as based on the unlawful attack made to his/her personality. However, the owner of the organization cannot demand compensation for the cancellation of the concerts, from the person who leaked the personal data. Although the causal relationship is established here, there is no "*relation of unlawfulness*". In addition, it should be expressed here that if the purpose of the person leaking the personal data of the singer is to cause damage to the owner of the organization, then the owner of the organization can file an action for compensation due to the immoral activity in the art. 49/2 of the TCO.

For the data subject to file an action for compensation against the data controller, he/she should have the capacity to sue. Natural persons with full capacity have the capacity to file any and all types of actions. If the data subject is a minor or restricted with the power of discernment, then he/she can file action for protection of the personal rights and action for moral compensation due to unlawful processing of the personal data, without the permission of his/her legal representative⁵⁹⁴. As a rule, the legal representative of these people cannot file these actions on behalf of them without taking the explicit or implicit consent of such minors or restricted⁵⁹⁵. However, the

⁵⁹¹ Oğuzman, Seliçi and Oktay-Özdemir, p. 250; Antalya, *Manevi Zararın Belirlenmesi*, p. 67.

⁵⁹² Tandoğan, p. 258; Oğuzman and Öz, Vol. II, p. 70.

⁵⁹³ According to *Tekinay*, relation of unlawfulness is the relation between the protection purpose of the violated rule of law and the violated benefit in order to be able to demand compensation. In other words, the damaging party shall be liable for the damage only when the violated rule of law's purpose is to protect. Tekinay, Akman, Burcuoğlu and Altop, p. 643; For detailed information about this, see: Kumru Kılıçoğlu, *Yansıma Yoluyla Zarar*, (Ankara:Turhan Kitabevi, 2012) p. 28 ff; Hatemi and Gökayla, p. 142; Oğuzman and Öz, Vol. II, p. 70; Antalya, *Manevi Zararın Hesaplanması*, p. 55.

⁵⁹⁴ According to *Eren* the demand for moral compensation is not a right which is tightly connected to the person, it is an ordinary receivable right and the authorization of the legal representative of the minor or restricted is required in order to file an action. Eren, p. 814.

⁵⁹⁵ Oğuzman, Seliçi and Oktay-Özdemir, p. 253; Tekinay, Akman, Burcuoğlu and Altop, p. 922.

legal representatives, although in a narrower scope, can file actions for the protection of the personal rights of the limited incompetent person in obligatory and urgent cases when the benefits of the limited incompetent person require so⁵⁹⁶. The action for material compensation on the other hand is filed by the legal representatives of these people⁵⁹⁷. The legal representatives of those who lack power of discernment can file any and all types of actions⁵⁹⁸.

In the LPPD, the information related to the legal persons are not accepted as personal data. Due to this reason, these are not protected within the scope of the LPPD. However, it is stated in the doctrine that the legal persons can also file actions for moral compensation as a result of an attack made to their social personal values⁵⁹⁹. Accordingly, if there is any attack to the social personal values of the legal person as a result of unlawful processing of the data related to the legal persons, then the legal persons can also file actions for moral compensation⁶⁰⁰.

⁵⁹⁶ Serozan, *Kişiler Hukuku*, p. 456; Ayözger, p. 299.

⁵⁹⁷ Tandoğan, p. 259.

⁵⁹⁸ Oğuzman, Seliçi and Oktay-Özdemir, p. 251; Eren, p. 814; The most important reason of this is that these people do not have the capacity to act on their own behalf and as a result the individuals who do not have full capacity are more likely to suffer violations. The individuals who lack full capacity shall be protected by their legal representatives who have the right to file actions for the protection of their personal rights. Gezder, *Türk Medeni Hukuku*, p. 40. According to Tekinay, for the individuals who lack mental capacity to file an action for moral compensation, the moral damages shall change as based on the selection of the objective opinion or the subjective opinion. If objective opinion is selected, the moral damage shall occur in case an attack is made to the personality of such person no matter how such person lacks the mental capacity, and such people shall also be able to file actions for moral compensation. However, in cases where the subjective opinion is acquired, the person lacking mental capacity due to mental disorder or mental defectiveness shall not be influenced psychologically or morally as a result of the attacks directed to such person's personality and accordingly, no moral damage shall arise. Due to this reason, such people cannot file actions for moral compensation. Tekinay, Akman, Burcuoğlu and Altop, p. 893.

⁵⁹⁹ Tekinay, Akman, Burcuoğlu and Altop, p. 893; Eren, p. 824; The legal persons are not protected since they do not have personal values such as life, health, bodily integrity, sexual freedom, which are specific to natural persons. However, the social personality values such as name, commercial reputation, honor, and respect, which are outside the personal values of natural persons, are protected for the legal persons. Gezder, *Türk Medeni Hukuku*, p. 49; Antalya, *Manevi Zararın Hesaplanması*, p. 68; Mine Kaya, p. 58.

⁶⁰⁰ Supreme Court ACC, D.01.02.2012, M. 2011/687, R. 2012/26. – Legalbank Elektronik Hukuk Bankası (Access Date: 10.02.2019); According to a decision of the Supreme Court dated, “*Since the rule of law recognizes the legal persons as a subject and since the personal values such as name, honor, dignity and reputation are given to them (art. 48 TCC), it shall be required to accept that the legal entities can also demand moral compensation. The moral damage is a damage which occurs not only in the presence of sorrow but also when the personal values of a person are attacked. Accordingly, both the Turkish Civil Code and TCO (Art. 49) protects not only the personal rights of the natural persons but also the personal rights of the legal persons. The written, oral or visual declarations humiliating the legal person's reputation, publications that such legal person lacks these or those qualities should*

3.1.2. Relatives of the Deceased Person

As a rule, the inheritors do not have the right to file an action in the attacks made to the personal rights⁶⁰¹. However, according to the dominating opinion accepted by the doctrine, some values related to the personality of the deceased person shall continue following the death⁶⁰². Due to this reason, it is accepted that the relatives of the deceased person can file actions for protection. What should be taken into consideration here is that it is not the inheritors who have the right to file this action, but the relatives of the deceased person. These people shall be able to file only the actions to protect the personality but they shall not have the right for compensation⁶⁰³.

As a rule, the moral compensation receivables do not pass to the inheritors⁶⁰⁴. However, the testator's inheritors can file an action for moral compensation if such testator had declared his will to demand moral compensation while he was alive⁶⁰⁵. This state is regulated in the art. 25/4 of the TCC as "*Claim for compensation of moral damages may not be transferred unless it is accepted by the counterparty; also, it may not be transferred to the heirs by way inheritance unless it is expressly declared by the testator*". The testator's declaration of will for claiming the moral damage can be in

be accepted to be an abuse of honor and dignity, which are personal rights. In addition to the legal person's honor and dignity, the social reputation, commercial reputation of such legal person also benefit from the protection provided by the 24th Article of the TCC." Supreme Court ACC, D.01.02.2012, M. 2011/4-687, R. 2012/26. – Legalbank Elektronik Hukuk Bankası (Access Date: 10.02.2019); For detailed information about the protection of the personal values of legal persons, see: Doruk Gönen, *Tüzel Kişilerde Kişilik Hakkı ve Korunması* (İstanbul: Onikilevha Yayıncılık, 2011).

⁶⁰¹ Petek, p. 41; According to *Serozan*, all the actions protecting the personal rights can be filed by the inheritors following the death of the injured party. Demand of only moral compensation cannot be claimed by the inheritors, unless the injured party claims it while he/she is alive. However, since the application of this rule today shall be outdated today, demand of moral compensation should be provided by using the limitation method in compliance with the purpose. *Serozan, Kişiler Hukuku*, p. 478; Eren, p. 814.

⁶⁰² Oğuzman, Seliçi and Oktay-Özdemir, p. 251; Antalya, *Manevi Zararın Belirlenmesi*, p. 67. According to Hatemi, only one personal value does not end by death. This is human dignity. Since it is a value which is related to the person, it is not transferred to the inheritors. The protection of this should be provided by the Government. Hatemi, p. 86.

⁶⁰³ Petek, p. 41.

⁶⁰⁴ Tekinay, Akman, Burcuoğlu and Altop, p. 924.

⁶⁰⁵ Hatemi, p. 79; Petek, p. 41. Oğuzman, Seliçi and Oktay-Özdemir, p. 251; Eren, p. 813.

the form of filing an action for compensation or declaration of the will by any manner whatsoever shall be sufficient for filing such an action⁶⁰⁶.

However, if material damage arises during the unlawful processing of the personal data, then the inheritors can file an action for compensation for compensating such damage⁶⁰⁷. This is because the inheritors have the right to claim factors with monetary value belonging to the personality⁶⁰⁸. The material compensation claims can also be transferred to others⁶⁰⁹.

3.2.Defendant

3.2.1. Natural Person Data Controller

Action for compensation should be filed against the person performing the activity resulting in the damage⁶¹⁰. The person mainly liable for the unlawful processing of the personal data is the data controller who determines the purposes and the means for processing the personal data. The data controller can be a natural person or a legal person. Two or more people can jointly determine the purpose and means of processing the personal data. In this case, according to the art. 26 of the GDPR both people shall be liable as the joint data controllers. According to the art. 61 of the TCO, if more than one person causes the occurrence of damage jointly, then the provisions related to the joint liability shall apply for them. In this case, the action can be filed against one, more than one or all of the joint controllers⁶¹¹.

In the actions for compensation filed by the data subject due to unlawful processing of the personal data, the defendant shall be the person with the capacity of the data controller, the data processor or their inheritors⁶¹². The claimant can file the action against any inheritor he/she desires.

⁶⁰⁶ Antalya, *Manevi Zararın Belirlenmesi*, p. 42; Eren, p. 813; Gezder, *Türk Medeni Hukuku*, p. 42. However,, according to Hatemi, claiming should be in the form of a declaration directed to the offender or his representative. Hatemi, p. 80.

⁶⁰⁷ Tandoğan, p. 259; Oğuzman and Öz, Vol. II, p. 70.

⁶⁰⁸ Oğuzman, Seliçi and Oktay-Özdemir, p. 252.

⁶⁰⁹ Tandoğan, p. 259.

⁶¹⁰ Oğuzman and Öz, Vol. II, p. 71.

⁶¹¹ Oğuzman and Öz, Vol. II, p. 71.

⁶¹² Oğuzman, Seliçi and Oktay-Özdemir, p. 252.

In strict liability, the defendant can be the person who has the liability⁶¹³. In case of processing performed by the data processor on behalf of the data controller and in employer's liability, the data controller shall be the defendant in the action for compensation to be filed, even if he/she did not perform the mentioned violation.

3.2.2. Legal Person Data Controller

3.2.2.1. Evaluation for the Private Law Legal Persons

According to the art. 50/2 of the TCC, the organs of the legal persons can put the legal person under obligation by "*legal transactions and all other activities*". According to this provision, the legal persons can perform legal transactions or tort activities through their organs authorized to represent⁶¹⁴. In other words, the organs of the legal persons cannot act as the performance assistant. This is because each activity of the authorized organs in compliance with the foundation documents shall be considered as the activity of the legal person. Due to this reason, if the personal data of the data subject are processed unlawfully by the organs of the companies, associations or foundations with legal personality, then the legal personality itself shall be liable for the damage to occur.

For the legal person to be liable for the activities performed by the organs of the legal personality, it is required that the person or persons acting with the capacity of an organ must perform the breach of obligation or tort while carrying out the works that are included within the frame of the activities of the organ of the legal person. For example, this is the case when an employee of a bank uses the credit information of the customers outside the field of activity of the bank and sells these to the third parties. The legal personality of the entity cannot be held liable for this. However, this can be considered within the scope of the employer's liability.

3.2.2.2. Evaluation for the Public Law Legal Persons

In some cases, the personal data of the individuals may be processed unlawfully by the public law legal person employees. In this case, to whom the data subject, whose personal data are unlawfully processed, shall direct the action of compensation?

⁶¹³ Eren, p. 825.

⁶¹⁴ In other words, the legal persons declare their wills through their organs. Hatemi, p. 113.

According to the art. 129/5 of the Constitution “*Compensation suits concerning damages arising from faults committed by public servants and other public officials in the exercise of their duties shall be filed only against the administration in accordance with the procedure and conditions prescribed by law, as long as the compensation is resorted to them.*” According to this provision, if the public servant processing the personal data unlawfully performed such processing during his duty by using his authorities, then the data subject shall not be able to file the action for compensation against him, even if he fulfills the conditions of tort liability⁶¹⁵. The data subject should file the action for compensation due to the damage suffered against the administration. The administration compensating the damage of the data subject shall be able to recourse it afterwards to the public servant who caused the damage by his fault⁶¹⁶. In this case, unlawful processing of the personal data constitutes the service fault. Accordingly, the public authority is required to compensate the mentioned damage whether or not it is faulty⁶¹⁷. If the employee is faulty, then it collects the compensation paid from the employee.

As a rule, although the damages caused by the public servants while performing their duties are considered as a service fault, the administration shall not always be directly liable for each activity performed by the public servant during his term of service. This is because if the activity performed by the public servant does not comply with the public service concept in any manner whatsoever, and if it can easily be discriminated from the conditions and boundaries of the duty, then the mentioned unlawful processing cannot qualify as a public service, even if performed during service. In this case, the data subject can directly file an action against the public servant⁶¹⁸.

⁶¹⁵ Oğuzman and Öz, Vol. II, p. 71;

⁶¹⁶ There is a special provision in the LPPD with respect to the public legal persons. According to the art. 18/3 of the LPPD, in violations where the data controller is a public legal person, the Board shall not be able to apply administrative fine to these legal persons. In place of this, disciplinary action is applied against the servants or the other public servants working in the public institutions, upon the notification to be made by the Authority. The decision to be taken as a result of the disciplinary action should be notified to the Board.

⁶¹⁷ Gürpınar, p. 691.

⁶¹⁸ According to the decision of the Supreme Court 4. CC., “*when it is taken into consideration that the compensation is demanded as based on the destruction of peace and comfort of the individuals by spread of the personal data without consent and that such activities cannot be considered within the scope of the content of the official duty of the defendant; the defendant’s personal fault which can clearly be separated from the duty was claimed and was the subject matter of the action. It is required*

4. LIABILITY OF SEVERAL PERSONS FOR THE SAME DAMAGE (JOINT AND SEVERAL LIABILITY)

In Turkish Law while partial liability is applied as a rule for the cases in which more than one person is liable for the damage to occur, joint and several liability is applied in some special cases stated in the law. According to the art. 61 of the TCO “*where several persons have together caused damage or are responsible for the same damage for different reasons, the provisions regarding joint and several liability shall be applied accordingly.*” Accordingly, in cases where several persons caused the damage together and cases where they are responsible for the same damage with different reasons, they are jointly and severally responsible for the mentioned damages⁶¹⁹. While each data controller causes the damage that occur (*joint data controllers*) in the first case, only one data controller causes the damage in the second case (*data controller – data processor*). The other or the others, although do not cause damage, are required to compensate the damage based on other legal reasons⁶²⁰.

Several persons can also be responsible for the material or moral damage to occur as a result of unlawful processing of the personal data. This case can be the result of unlawful data processing by the joint data controllers within the scope of the protection of personal data or the result of the unlawful data processing carried out by the data processor acting on behalf of the data controller. Or unlawful processing of the personal data of the third parties during the performance of the data controller’s employees shall result in joint and several liability.

In the art. 82/4 of the GDPR it is clearly stated that the damage of the data subject shall be compensated as based on the joint and several liability provisions in cases where there are more than one controller for the same processing or where both a controller and a processor are involved in the same processing⁶²¹. In the art. 12 of the LPPD it is

for the court to accept that hostility can be directed to the defendant and to settle the basis of the disagreement.” see: Supreme Court, 4CC., D.24.11.2014, M. 2014/11608, R. 2014/15800. - Legalbank Elektronik Hukuk Bankası (Access Date: 22.03.2019).

⁶¹⁹ Eren, p. 834; Oğuzman and Öz, Vol. II, p. 299.

⁶²⁰ Eren, p. 834.

⁶²¹ In the art. 82/4 of the GDPR, it is stated that “*Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.*”.

stated that in case of the unlawful processing of the personal data by a natural or legal person on behalf of the data controller, or in case of not providing the data security, then the data controller shall jointly be responsible with these persons.

4.1.The Liability of the Joint Data Controllers

The joint data controllers performing the personal data processing activity jointly⁶²² shall jointly and severally be responsible for the damage to occur in case of an unlawful processing activity. Joint and several liability is the state of liability of several persons for the same damage⁶²³. Joint and several liability of the joint data controllers is based on causing the same damage jointly⁶²⁴.

For example, the joint and several liability of the data controllers shall arise if the personal data of a data subject are accessed by the third parties without the consent of the data subject due to not taking the required security measures stated in the law, by the joint data controllers, after the lawful processing of the personal data within the frame of a contract. Here, each data controller shall be liable due to the same reason, which is the violation of the contract. In such a case, the data subject can claim the compensation of the damage to occur, from all the joint data controllers in compliance with the joint and several liability provisions. In compliance with the art. 82/2 of the GDPR⁶²⁵ it is stated that “*Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.*”

⁶²² Although the joint data controllers are not regulated in a separate provision in the LPPD, there are cases in practice in which several persons determine the purposes and means of processing the personal data. Due to the frequent nature of this state, two or more data controllers jointly determining the purposes and means of processing are called joint data controller in compliance with the article 26 of the Regulation. For detailed information about this subject, see: Alsenoy, p. 280.

⁶²³ Kılıçoğlu, *Genel Hükümler*, p. 575.

⁶²⁴ This state is called common fault in the doctrine. Common fault occurs when more than one person knowingly and intentionally contributes to the same event or state that causes damage. Alsenoy, p. 281. For detailed information about common fault, see: Oğuzman and Öz, V.II, p. 300.

⁶²⁵ In the Directive no 95/46/EC, there is no regulation concerning how the joint data controllers shall share the legal liabilities. The only regulation concerning this issue is the statement given by the European Commission at the preparatory stage of the Directive 95/46/EC. Accordingly, “*each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed*”. COM (95) 375 FINAL-cod287, “Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, p. 3. For the report, see: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51995PC0375&from=EN> (Access Date: 10.02.2019).

For the joint data controllers to be jointly and severally liable for the damage to arise, it is sufficient that they cause the damage jointly. The extent of their effect in the occurrence of the mentioned damage or the role they played or their duties in the processing activities are not important with respect to the joint and several liability⁶²⁶. In any case, the data subject can demand the compensation of the damage suffered, from all the joint data controllers who cause such damage⁶²⁷. Each one of the joint data controllers shall be held liable for the whole entire until the whole damage of the data subject is compensated. This is regulated in the art. 82/4 of the GDPR as “*each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject*”. For these people to be liable for the whole damage, they are required to perform the same processing activity and to bear the liability conditions for the damage due to the processing activity, in compliance with the 2nd and 3rd paragraphs of the same article. According to the art. 166/1 of the TCO, where one joint and several data controller compensates the damage of the data subject, the other joint data controllers are discharged of their liabilities against the concerned data subject.

According to the art. 82/5 of the GDPR, the data controllers or the data processor after paying the full compensation for the damage suffered by the data subject, shall be entitled to claim back from the other data controllers or data processors involved in the same processing, that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph⁶²⁸. This regulation is in compliance with the joint and several liability provisions of the TCC. Joint data controllers may regulate the method for sharing the liabilities for internal relations (*internal allocation*) by a joint data controllers contract to be concluded⁶²⁹. This contract eliminates uncertainties concerning how the liabilities and obligations shall be shared and provides a clearer and net sharing. However, in any case, the liability shall be shared as based on the requirements of the

⁶²⁶ Kılıçoğlu, *Genel Hükümler*, p. 578.

⁶²⁷ Kılıçoğlu, *Genel Hükümler*, p. 578.

⁶²⁸ The provision of the art. 82/5 of the GDPR is regulated as; “ *Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.* ”.

⁶²⁹ Alsenoy, p. 281.

factual circumstances. This is because sometimes the provisions in the contract may not reflect the factual circumstances.

4.2.The Liability of the Data Processor

If the data controller does not authorize the data processor for processing the personal data, how to share the liability, whether or not the liability shall also be transferred together with the transfer of the authority were the arguable issues. It should be expressed here that although the data processor processed the personal data, he/she is required to act in compliance with the instructions of the data controller during such processing activities. As a result, it cannot be said that the data processor is independent of the data controller with respect to this⁶³⁰.

The first provision to come to mind with respect to the liability arising of the unlawful activities of the data processor is the art. 12/2 of the LPPD. According to this provision, *“In case of the processing of personal data by a natural or legal person on behalf of the controller, the controller shall jointly be responsible with these persons for taking the measures laid down in the first paragraph.”* Together with this provision, if the data controller authorizes a third party for the data processing activity, it is apparent that the data controller shall have strict liability for the unlawful activities performed. In this case, the data controller, although has no fault, shall have joint and several liability with the data processor for the external relation⁶³¹. The data subject can file an action directly against the data processor for the elimination of the damage as well as the data controller. Since the art. 12/2 of the LPPD is a mandatory provision, this liability cannot be eliminated with the personal data processing contract which is concluded by the parties⁶³².

Due to this reason, when the data processor performs the personal data processing activities on behalf of the data controller, if unlawful processing is performed, then the data subject can demand both the data processor and the data controller to compensate the damage. In this case, while the data processor is liable in person for the damage to

⁶³⁰ Dülger, p. 21.

⁶³¹ This state is an example to being liable for the same damage for various reasons, which is a type of joint and several liability regulated in art. 61 of the TCO. Accordingly, several persons are responsible for compensating a damage suffered by one person, due to different legal reasons. Oğuzman and Öz, Vol. II, p. 300.

⁶³² Taştan, p. 131.

occur, the obligation for compensating the damage arises according to the art. 12/2 of the LPPD, even if the data controller does not cause the occurrence of the damage. Accordingly, although one of the parties is liable for the damage that arises, many persons shall be liable against the injured party for compensation of the damage due to the different legal reasons.

In the art. 82 of the GDPR, it is stated that both the data controller and the data processor shall be liable for the material and moral damages to occur in case of violation of the Regulation⁶³³. According to the art. 82/2 of the GDPR, the data processor has to either violate the obligations of the data processor regulated by the Regulation or act contrary to the legal instructions given by the data controller for the liability to arise with respect to the unlawful processing of the data. In cases where the data processor is liable, the data controller shall also be liable for the damage to occur, as well as the data processor according to the 3rd paragraph of the same article. However, they can only be relieved of the liability if they prove that they are not liable for the events giving rise to the damage in any manner whatsoever⁶³⁴.

For example, Company A operating in the field of clothing sector desires to send advertisements to the customers by mail within the scope of the consent taken from the customers. For this purpose, Company A concludes an agreement with Company B which is specialized and experienced institution in this area. Company B sends information mails concerning the campaigns of the Company A at certain intervals within the direction of Company A's instructions. However, if the e-mail addresses of the customers are stolen and are acquired by the third parties as a result of security weakness of the Company B, who acts in its capacity as the data processor, both the data controller Company A and the data processor Company B shall be jointly liable for the whole damages of the data subjects to arise, regardless of their degrees of the fault or their roles in the data processing activities

⁶³³ Ayşe Nur Akıncı, p. 14; Çekin, *Kişisel Verilerin Korunması*, p. 80; There is no provisions concerning the liability of the data processor in the Directive No 95/46/EC. These provisions arranging the liabilities of the data controller and the data processor are very important for eliminating the uncertainties on how to share the liability between the data controller and the data processor.

⁶³⁴ According to the art. 82/3 of the Regulation; "*A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.*"

4.3.Data Controller’s Liability as an Employer

In practice, usually the data controllers assign the personal data processing activity to their employees or the third parties. For example, a bank performs the personal data processing required by the banking activities through its employees. Or when Company X prepares the personal files of its employees, the employees in the human resources department process the personal data of such employees. The strict liability of the data controller occurs when the employees damage a third party during the personal data processing activities performed on behalf of the data controller. According to the art. 66/1 of the TCO is as “*An employer has to compensate the damage caused to the others by his employee in the performance of the work given to him.*” This provision shall be applied when data controller, as the employer, assigns the processing activities to others⁶³⁵.

Accordingly, the law imposed the duty of care on the data controller when he/she assigns the employees to perform the personal data processing activities, on behalf of the data controller. In case the employers cause damage to a third party while this activity, it is presumptively accepted that the data controller have acted against the mentioned duty of care⁶³⁶. The duty of care required by the law is not a subjective obligation changing according to the data controller, but it is an objective obligation⁶³⁷. The main reason for the law to impose such an obligation on the employer is that it shall be more *equitable* for these people to compensate the damages caused by the

⁶³⁵ Within the scope of the art. 66 of the TCO, the following conditions should be realized in order for the occurrence of the strict liability of the data controller, as the employer. a) The damaging party is required to be the employee of the data controller. b) The damage should occur as a result of unlawful behavior during the performance of the work by the employee. c) The damage is required to be suffered by a third party who is not a party to the contract. d) The data controller should have not been able to bring proof of salvation. Accordingly, if the data controller proves that he/she had shown due care and paid due attention objectively, then he/she shall be relieved of the liability. For detailed information, see: Tandoğan, p. 106 ff.; Seda Kara Kılıçarslan, *Adam Çalıştırmanın Sorumluluğu*, (Ankara: Turhan Kitabevi, 2017), p. 67 ff.

⁶³⁶ Oğuzman and Öz, Vol. II, p. 149.

⁶³⁷ Tandoğan, p. 118; Kılıçarslan, p. 84.

people employed by them, who work under the employer's dominance and within the direction of the employer's benefits⁶³⁸.

Due to this reason, it shall not be sufficient to prove his/her faultlessness for the data controller, in his capacity as the employer, to be relieved of liability. The data controller is required to bring evidence of salvation mentioned in the art. 66 of the TCO. According to this provision, if the data controller proves that he/she had fulfilled the duty of care in order to prevent the damage, when choosing the employee, giving instructions concerning the work, supervising and controlling, then he/she will be able to be relieved of the liability⁶³⁹. The data controller is required to prove that he has a right to believe that the persons processing the personal data or providing the data security are qualified for such activities and that he/she provided the required information in order to such damages when instructing for the mentioned activities and to perform the controls during the work activities of the employee. The data controller's obligation to provide the control of the employee can be derived from the art. 14 of the LPPD. It is stated in the art. 14/3 of the LPPD as "*The controller shall be obliged to conduct necessary inspections, or have them conducted in his own institution or organization, with the aim of implementing the provisions of this Law.*".

Another obligation imposed by the law for relieving the data controller from the liability to arise of the damages caused by the employee is the burden of proof that the work order of the entity is made appropriate for the prevention of the occurrence of the damage⁶⁴⁰. The data controller is required to take any and all technical and administrative measures for the lawful processing and access of the data within the entity's organization and for the storage of such data⁶⁴¹.

⁶³⁸ Oğuzman and Öz, Vol. II, p. 142. The opinions constituting the basis of the employer's liability are equity, benefit, cause, dominance and risk opinions. For detailed information about these opinions, see: Kılıçarslan, p. 16 ff.

⁶³⁹ Tekinay, Akman, Burcuoğlu and Altop, p. 685.

⁶⁴⁰ According to the art. 66/3 of the TCO, "*An employer has to compensate the damage caused within the sphere of the activities of an enterprise, unless he proves that the organization of such enterprise was appropriate to avoid the occurrence of a damage of this type.*"

⁶⁴¹ This state is regulated by the art.14/1 of the LPPD. On the other hand, the measures that can be taken by the data controller in order to prevent the occurrence of damage as a result of the data processing activities are specifically regulated in the GDPR. The obligations imposed on the data controller such as the principle of transparency (art.5 /1), accountability (art. 5/2), data protection by default and data protection by design (art. 25), data protection, appointment of data protection officer (art.37) and data protection impact assessment (art.3 5) can be given as the examples to this.

The art. 66 of the TCO is applied to the employers within the scope of the provisions of the private law. The employer can be a natural person as well as a legal person. What is important here is that the work relation should take place within the frame of the provisions of the private law. For example, bank A has given its employee, who is employed within the scope of a labor contract, the authority to use the credit rating program in order to assess the creditability of the customers. If the mentioned employee uses this program for different purposes and learns the financial data of a third party and then damages such third party as a result of this information acquired, then the bank A, which is the data controller shall be liable within the frame of the art. 66 of the TCO.

However, the employer public law legal entity shall be liable in compliance with the provisions of the public law for the damages caused to the 3rd parties during the processing activity of the State or public legal entity and the employees employed as being subject to the provisions of the public law⁶⁴². Due to this reason, if the employer was the Ministry A in place of the bank A in the example given above, and if the person performing the processing activity of the ministry was an employer in the position of public servant, then the provisions of the art. 66 of the TCO would not be applied. Finally it should be expressed here that the public legal entities are liable for the damages caused by the employees employed within the frame of the provisions of the private law, within the scope of the employer's liability⁶⁴³.

In cases where the data controller is a legal person, the activities performed by the organs of the data controller by representation of the legal person shall be considered as the activities of the legal person and accordingly, these shall not be considered within the employer's liability. In this case, the legal person itself shall directly be responsible for the activities of the organs⁶⁴⁴. According to the art. 50/3 of the TCC, both the legal entity and the organ performing such activity are liable against the injured party directly in compliance with the art. 49 of the TCO. The legal entity and the organ shall be held jointly and severally for the damage to occur⁶⁴⁵. However, fault

⁶⁴² Tekinay, Akman, Burcuoğlu and Altop, p. 680; Eren, p. 648; Oğuzman and Öz, Vol. II, p. 143.

⁶⁴³ Eren, p. 648; Tekinay, Akman, Burcuoğlu and Altop, p. 682.

⁶⁴⁴ Tekinay, Akman, Burcuoğlu and Altop, p. 680; Oğuzman and Öz, Vol. II, p. 62.

⁶⁴⁵ Oğuzman and Öz, Vol. II, p. 149; Eren, p. 649.

is sought here in order to hold the legal entity and the organs of the legal entity liable within this frame. On the other hand, the fault of the data controller is not sought in the employer's liability⁶⁴⁶.

The data controller's liability as the employer does not mean that he/she shall not be liable for the damages to occur due to the unlawful processing of the personal data as a result of employee's fault or as a result of not providing the data security. The data controller's employee shall be liable for the damages to occur as a result of the processing activity to the extent of his/her fault⁶⁴⁷. While the person with the capacity of a data controller is liable in compliance with the provision of the strict liability regulated by the art. 66 of the TCO, the employee is liable for the tort committed by himself/herself. In this case, there shall be liability for the same damage for different reasons, which is a type of joint and several liability. The data controller has the right to recourse the compensation paid to the extent the employee is personally liable for the occurrence of the damage.

5. STATUTE OF LIMITATION IN THE ACTION FOR COMPENSATION

Following the determination of the compensation amount, although the mentioned compensation demand is converted into the right to claim, the statute of limitation for the material and moral compensation demands arising of the tort is regulated specifically by the art. 72 of the TCO. Accordingly, the statute of limitation for the compensation demands is different from the provision of statute of limitation regulated in the art. 146 of the TCO concerning the contractual rights to claim⁶⁴⁸. This difference is due to the start and term of the statute of limitation. The general provisions of the statute of limitation are applied jointly in the issues such as the stop and interruption of the statute of limitation⁶⁴⁹.

⁶⁴⁶ Tandoğan, p. 125.

⁶⁴⁷ Tekinay, Akman, Burcuoğlu and Altop, p. 689.

⁶⁴⁸ Mehmet Erdem, *Özel Hukukta Zamanaşımı* (İstanbul: Onikilevha Yayıncılık, 2010), p. 123; Eren, p. 855.

⁶⁴⁹ Şahin Akıncı, p. 189.

5.1. Statute of Limitation Arising of the Contractual Relation

According to the art. 146 of the TCO, the statute of limitation in the actions for compensation based on the breach of obligation is ten years, unless there is a contrary provision in the law⁶⁵⁰. If the damages due to the unlawful processing of the personal data or not taking the sufficient security measures constitute breach of obligation, then the term for the statute of limitation is calculated as ten years, as a rule⁶⁵¹. For example, if the personal data of a data subject are unlawfully processed via service contract, the data subject with the capacity of the employee can file an action for material or moral compensation within a term of ten years as of the occurrence of the breach of obligation.

5.2. Statute of Limitation Arising of the Tort Relation

If the liability giving rise to an action for compensation is arising of tort liability, then according to the art. 72 of the TCO, it is two years starting from the date on which the injured party becomes aware of the damage and the person liable for the compensation and in any event, it is ten years after the date on which such activity is performed⁶⁵². Although this is the rule, if longer term of statute of limitation is provided in the penal laws for the activity causing such compensation, then such statute of limitation is applied. Accordingly three different terms are required to be taken into account in the actions for compensation to be filed.

5.2.1. Normal Term

The data subject to file an action for compensation against the data controller as a result of unlawful processing of the personal data should file it within 2 years as of the

⁶⁵⁰ According to an opinion in the doctrine, since it is accepted that the compensation demand arising of the breach of obligation is a different form of the debt obligation that became impossible, it is accepted that the actual obligation is subject to the statute of limitation. Tekinay, Akman, Burcuoğlu and Altop, p. 854; According to Oğuzman, the compensation liability of any type of the breach of obligation occurs as a new obligation. Due to this reason, it is subject to ten years of statute of limitation in compliance with the art. 146 of the TCO, unless there is a contrary provision in the law. Oğuzman and Öz, Vol. I, p. 433.

⁶⁵¹ If an attack made to the personality, is made within the frame of a contractual relation, then this term for the statute of limitation shall be subject to the term of the statute of limitation for the contractual claims. Erdem, p. 131.

⁶⁵² These terms stated in the law shall apply both for the material compensation and the moral compensation claims. Erdem, p. 123.

date on which the data subject becomes aware of the damage occurring as a result of the unlawful processing activity and the identity of the data controller. Otherwise, the compensation demand shall be time barred. However, if the data subject whose personal data are processed is minor or restricted, then this term shall start on the date when the legal representative of the data subject becomes aware of the material damage and the identity of the data controller⁶⁵³. On the other hand, since the action for moral compensation can be filed by the minors with the power of discernment without the consent of the legal representative, the statute of limitation term of two years starts as the data subject becomes aware of the damage and the identity of the data controller.

If there are several data controllers processing the personal data unlawfully, learning their identity by the data subject is important for the start of the term⁶⁵⁴. For example, a travel agency and airline company formed a joint internet platform. This way, they achieve better cooperation concerning the travel data of the customers⁶⁵⁵. In this case, when the personal data of the data subject accessing that website are processed unlawfully, the action for compensation shall start separately as of the date on which the data subject becomes aware of each data controller. If the data subject becomes aware of the fact that the travel agency has processed his/her personal data unlawfully but did not file an action by the end of 2 years, and if becomes aware of the fact that the airline company is also liable for the compensation on the 3rd year, then the term of 2 years of statute for limitation applies against the airline company.

In cases where the tort is continuous, neither the term of 2 years nor the term of 10 years start before the termination of the activity⁶⁵⁶. For example, the term for the statute of limitation shall not start against the data controller processing the personal data unlawfully during term in which such data are held by him/her. This is because the tort is continued to be committed each moment the data acquired unlawfully are kept.

⁶⁵³ Supreme Court, 11.CC., D.17.04.1975, M. 1975/443, R.1975/1975. - (Legalbank Elektronik Hukuk Bankası); Oğuzman and Öz, Vol. II, p. 73.

⁶⁵⁴ Oğuzman and Öz, Vol. II, p. 73.

⁶⁵⁵ Article 29 Data Protection Working Party, *The Concepts of "Controller" and "Processor"*, p. 20.

⁶⁵⁶ Erdem, p. 179; Oğuzman and Öz, Vol. II, p. 75; Supreme Court, 4.CC., D.08.03.2005, M. 2004/5114, R. 2005/2290. - (Legalbank Elektronik Hukuk Bankası).

Moreover, if a new damage, which cannot be predicted by the data subject, arises as a result of processing the personal data then “2 years of statute of limitation” shall start to apply as of the moment such damage is noticed, if the maximum term of ten years have not lapsed⁶⁵⁷.

5.2.2. Maximum Term

According to the art. 72/1 of the TCO, the right to file an action due to tort is 10 years in any case, as of the date on which the damaging activity is committed. Accordingly, whether the injured party became aware of the damage and the person liable for the compensation is not taken into consideration. Due to this reason, if the person whose personal data are unlawfully processed, becomes aware of the data controller and the damage 10 years after the processing date, his/her right to file an action for compensation shall be subject to statute of limitation.

The date that is significant for the term of 10 years is the date on which the tort is committed. The damage may occur after a certain time following the commitment of the tort activity. In other words, the date on which the term of 10 years starts is not the date on which the damage occurs, but the date on which the activity causing the damage is completed⁶⁵⁸. What is important is the date on which the tort is committed. For example, the data controller (A) who is required to protect the personal data leaked the bank data of (B) as a result of not paying due care and attention. However, (C) who unlawfully acquired such data waited for some time so that things calm down and after one year, accessed (B)’s account and took the money in the account. In this case, the statute of limitation term of 10 years shall start on the date on which the data are leaked, even if the damage takes place 1 year later.

5.2.3. Exceptional Term

In cases such as unlawful recording, transfer, sharing, acquisition or non-destruction of the personal data, the action for compensation to be filed due to such activities shall be subject to the statute of limitation applicable for the penal actions according to the

⁶⁵⁷ Oğuzman and Öz, Vol. II, p. 75.

⁶⁵⁸ Erdem, p. 135; Oğuzman and Öz, Vol. II, p. 76.

art. 72/2 of the TCO since these activities constitute a crime⁶⁵⁹. This term starts as of the date on which the activity which should be considered as a crime, is committed⁶⁶⁰.

According to the article 66 of the TPC, “*in offenses requiring punishment of imprisonment or punitive fine not more than five years*” the term for the statute of limitation for the penal actions is provided as 8 years. Accordingly, maximum term of 10 years in art. 72 of the TCO shall continue to be effective since the term of statute of limitation for the penal action is shorter than 10 years⁶⁶¹. However, the two-year term of the statute of limitation shall also be effective after the lapse of the statute of limitation of the penal action. Due to this reason, even if the data subject becomes aware of the data controller and the damage during the penal trial, he/she shall have the right to file an action within two years after the lapse of 8 years. For example, according to the art. 136 of the TPC, “*Anyone who imparts to others, distributes or acquires personal data unlawfully shall be punished by imprisonment for a term of from two to four years.*” In this case, action for compensation based on the private law can be filed against the person who processed the personal data lawfully, but then shared such data with the third parties without the consent of the data subject. Accordingly, the data subject can file an action for compensation until the end of the statute of limitation of the penal action. Following the end of the statute of limitation of the penal action, the statute of limitation with a term of 2 years shall start and the action for compensation can be filed on these dates.

However, in cases where this crime is a major crime, the punishment to be given shall be increased by half. Accordingly, the statute of limitation for the penal action is regulated as fifteen years based on the art. 66 of the TPC. As a result, the term for the statute of limitation within this frame is fifteen years in any case, as of the date on which the tort is committed.⁶⁶²

⁶⁵⁹ Supreme Court, 17.CC., D.30.09.2015, M. 2015/9926, R. 2015/9931. – Legalbank Elektronik Bilgi Bankası, (Access Date: 15.05.2019); Supreme Court, 19.CC., D. 23.11.1992, M. 1992/20267, R. 1992/6169; Supreme Court, 4.CC., D.05.03.1990, M. 1989/7450, R. 1990/1920. – Legalbank Elektronik Bilgi Bankası, (Access Date: 15.05.2019).

⁶⁶⁰ Oğuzman and Öz, Vol. II, p. 77.

⁶⁶¹ Oğuzman and Öz, Vol. II, p. 77.

⁶⁶² Ayözger, p. 304.

Another important issue to be mentioned here is that the statute of limitation of the penal action shall apply only for those who commit activities that constitute crime⁶⁶³. In some cases, there may be individuals whose activity does not constitute a crime, although he/she is liable for compensation for the same activity but for a different legal reason. For example let's think (A) working in (X) telecommunication company clandestinely records the telephone calls and then blackmails the customers as based on these telephone conversations. In this case, (X) telecommunication company shall be liable according to the private law in compliance with the provision of the art. 116 of the TCO. Due to this reason, the customers can file actions for compensation against X company by taking into consideration the statute of limitation terms of the private law. However, since (A)'s activity constitutes a crime, the statute of limitation for the penal action shall be significant for the action for compensation to be filed against (A).

6. AUTHORIZED AND COMPETENT COURT IN THE ACTIONS FOR COMPENSATION

As a rule, the competent courts are the civil courts in the actions for compensation where there is private law liability. In cases where the activities of processing and recording of the personal data also constitute a crime, the compensation of the damages arising of the private law is determined by the civil courts, even if a public action is filed and the criminal judgment is carried out by the penal court⁶⁶⁴.

As a rule, the authorized court in the action to be filed before a civil court is the court in the domicile of the defendant (art. 6 of CCP). Since unlawful processing of the personal data constitutes tort, the place where such processing is performed or the

⁶⁶³ Oğuzman and Öz, Vol. II, p. 79. However, there are some decisions contrary to this opinion in some Supreme Court decisions. According to Supreme Court 17. CC decision, “...in the mentioned provision, no discrimination is made between the driver and others liable (for example the operator) concerning the application of the statute of limitation for the penalty, and accordingly, it is stipulated that the rule applies to all these cases and that the same term of statute of limitation would be applied...” Supreme Court, 17.CC., D.30.09.2015, M. 2015/9926, R. 2015/9931. – Legalbank Elektronik Hukuk Bankası, (Access Date: 15.05.2019); Supreme Court 17. CC., D.26.03.2015, M. 2015/304, R. 2015/4919. – Legalbank Elektronik Hukuk Bankası, (Access Date: 15.05.2019).

⁶⁶⁴ According to the prior Law of Criminal Procedure no 1412, if the injured party had filed a personal case before the penal court in cases where the tort constitutes a crime, or intervened the public action and demanded compensation, then the court could have convicted the accused to compensation. This state was changed with the Code of Criminal Procedure no 5271.

place where the damage took place or the domicile of the injured data subject courts are also authorized.

7. EFFECT OF THE PENAL COURT DECISION ON THE ACTION FOR COMPENSATION

Violation of the personal rights of a person due to the unlawful processing of the personal data is usually considered as a crime in compliance with the provisions of the articles 135-140 of the TPC⁶⁶⁵. In this case, the penal action can continue beside the action for compensation to be filed before the civil courts. The effect of the penal court decisions on the private law judgments is regulated in the art. 74 of the TCO⁶⁶⁶.

According to the first paragraph of this article, the judge trying the case “*when determining fault or lack of fault and capacity or incapacity to consent, is not bound by the provisions governing criminal capacity*”⁶⁶⁷. Since the fault or the power of discernment criteria sought in the penal judgment differ, the judge of the action for compensation shall decide as based on the principles of Civil Code concerning these

⁶⁶⁵ For detailed information about the comparison of the penal liability and the private law liability, see: Kadir Berk Kapançı, “Ceza Mahkemesi Kararlarının Hukuk Mahkemesi Kararlarına Etkisi”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, Vol. VII (2016), p. 1; Hatemi and Gökyayla, p. 115; Tekinay, Akman, Burcuoğlu and Altop, p. 946.

⁶⁶⁶ This provision applies when the activities constituting tort are also a crime. For detailed information about the relation between tort and crime, see: A. İsmet Arslan, “Ceza Hukuku Kurallarının Haksız Fiilden Doğan Tazminat Taleplerine Etkisi (I)”, *Yargıtay Dergisi*, Vol. VI, Issue. 1-2 (January- April 1980), pp. 157-178.

⁶⁶⁷ This provision enables private law judge to act freely against the penal judgment. This is called “*the principle of independence*” in the doctrine. Arslan, *Tazminat Taleplerine Etkisi (I)*, p. 167; Kapançı, p. 515; Ahmet Kılıçoğlu, “Haksız Fiillerden Sorumlulukta Ceza Hukuku İle Medeni Hukuk İlişkisi”, *AÜHFD*, Vol. XXIX, (1973), p. 191; However, this independence is not absolute since the penal judgment decisions bind the private law judge in some cases.

issues⁶⁶⁸. The civil court judge is likewise not bound by the verdict in the criminal court⁶⁶⁹.

In cases where the unlawful processing of the personal data constitutes a crime, the penal court's decision for acquittal also does not bind the judge trying the action for compensation. If the reason of the decision for acquittal given by the penal court is based on the fact that the activity does not constitute a crime or that there is no causal relationship⁶⁷⁰, then there shall be no arguments with respect to the mentioned decision⁶⁷¹. This is because the activities which do not constitute a crime may be considered as tort with respect to the compensation law. What is discussed in the doctrine concerning this issue is whether this shall bind the private law judge in the decisions of acquittal related to the fact that the accused did not commit the crime

⁶⁶⁸ Oğuzman and Öz, Vol. II, p. 83; In penal judgment, although the civil court judge is not bound by the verdict, for the civil court being bound by the material fact determined by the penal court both in the scientific and rooted judicial decisions, see: Supreme Court, 4.CC., D.04.05.2016, M. 2015/6951, R. 2016/6080. - Legalbank Elektronik Hukuk Bankası, (Access Date: 23.03.2019). The fault criteria in the Penal Court and the fault criteria of the Civil Code are assessed differently. This is because the Penal Code seeks intention for most of the crimes while intention or negligence is sufficient for the liability arising of tort in the Civil Code. The offender may be held liable without any fault in some cases of strict liability. Tekinay, Akman, Burcuoğlu and Altop, p. 947; Antalya, *Manevi Zararın Belirlenmesi*, p. 64.

⁶⁶⁹ Kılıçoğlu, *Ceza Hukuku İle Medeni Hukuk İlişkisi*, p. 197; Tekinay, Akman, Burcuoğlu and Altop, 950.

⁶⁷⁰ In penal law, the formation of crime causal relationship is subject to stricter conditions. Due to this reason, the decision that the causal relationship could not be formed in the penal judgment does not bind the civil court judge. However, if the penal judge establishes a causal relationship between the damaging activity and the damage, then this decision binds the civil code. Tekinay, Akman, Burcuoğlu and Altop, p. 953; Kılıçoğlu, *Ceza Hukuku ile Medeni Hukuk İlişkisi*, p. 199; However, according to *Kapanıcı*, since no reasoning can be made about the damage with the verdict of the penal court, the civil court judge shall not be bound in any case, whether or not the causal relationship is formed in the conviction decision. *Kapanıcı*, p. 532. For the decisions of the Supreme Court concerning the fact that the determination of the causal relationship in the conviction decision of the penal court binds the civil court judge also, see: "...It is derived from the documents available in the file that the defendants are being tried before Bilecik High Penal Court due to the event that constitutes the subject matter of the action, and that were convicted of the crime of neglect of duty, but this decision is at the stage of appeal and not finalized yet. In compliance with the article 53 of the Code of Obligations, **the unlawfulness of the activity in the decision for conviction given by the penal court and the binding nature for the civil court judge of the acceptance concerning the material events determining the causal relationship are accepted both under the scientific opinions and the judicial decisions. In this case, the finalization of the penal case which is at the stage of appeal should be waited...**" Supreme Court, 4. CC., D.15.12.2015, M. 2015/16972, R. 2015/13599.

⁶⁷¹ *Kapanıcı*, p. 518; Oğuzman and Öz, Vol. II, p. 83.

attributed to him⁶⁷². However, if the reasoning of the decision for acquittal is insufficient evidence concerning the crime, then such decision for acquittal shall not bind the civil court judge⁶⁷³.

If the penal court decided the conviction of the accused, then this decision binds the private law judge with respect to the material event⁶⁷⁴. This state, is also understood from *a contrario* of the provision of the law⁶⁷⁵. However, the parts related to the fault and the degree of fault accepted in the decision given for the conviction by the penal court shall not constitute a proof positive in the private law judgment⁶⁷⁶. In other words, the penal court judge's decision for the fault shall not bind the civil court judge with respect to the assessment of the fault⁶⁷⁷. If there is a part in the decision of the penal court concerning the damage, it is also stated in the art. 74/2 of the TCO that *the decision of the penal court with respect to the determination of the damage shall not bind the civil court judge*.

The final point to be emphasized here is that if an action for compensation is filed before a civil court while the penal judgment continues, the civil court judge can give decision with respect to the compensation without waiting for the decision of the penal court⁶⁷⁸.

8. COMPETITION OF THE CONTRACT AND TORT RELATION

If there a contract exists in unlawful processing of the personal data, the data contractor's contractual liability and the tort liability shall compete⁶⁷⁹. In cases where

⁶⁷² For those who think this is binding, see: Tekinay, Akman, Burcuoğlu and Altop, p. 951; Kılıçoğlu, *Ceza Hukuku ile Medeni Hukuk İlişkisi*, p. 199; Kapancı, p. 534.

⁶⁷³ Kılıçoğlu, *Ceza Hukuku ve Medeni Hukuk İlişkisi*, p. 198.

⁶⁷⁴ If the penal court judge determined during the penal judgment that the factors of the activity are completed and committed (that the material event took place), that the mentioned activity is unlawful and that the parties performed the mentioned activity and decided accordingly, then this decision constitutes a proof positive for the private law judgment. Kapancı, p. 521.

⁶⁷⁵ For the Supreme court decisions concerning that the decision of conviction of the penal court shall bind the private law judge during the private law judgment, see: Supreme Court, 15. CC., D.25.12.2008, M. 2008/5310, R. 2008/764. – Legalbank Elektronik Hukuk Bankası, (Access Date: 20.03.2019).

⁶⁷⁶ Tekinay, Akman, Burcuoğlu and Altop, p. 949; Oğuzman and Öz, Vol. II, p. 84; Kapancı, p. 527.

⁶⁷⁷ Tandoğan, p. 350; Kapancı, p. 527.

⁶⁷⁸ Oğuzman and Öz, Vol. II, p. 85.

⁶⁷⁹ In some cases, breach of obligation also has the nature of tort and if the debtor may apply to tort provisions or breach of contract provisions as he/she desires. However it should be expressed here that,

more than one right is violated with the same activity, if the result of more than one demand that can be claimed cannot be added onto each other, this shall give rise to the competition of claims⁶⁸⁰.

Due to this reason, the person whose personal rights are violated due to unlawful processing of the personal data cannot demand compensation due to tort on one side and compensation due to the breach of obligation on the other side. Otherwise, more than one compensation shall be decided due to the same material and moral damage. This does not comply with the justice purpose of the law. The art. 60 of the TCO is regulated in order to solve this problem. According to this provision, “*Where one person is liable for the same damage on different legal grounds, the judge shall consider the legal ground which permits the most favorable compensation for the injured person, unless the latter claims otherwise or there is a contrary provision.*”

According to the mentioned provision, if an unlawful activity constitutes both the breach of obligation and tort, then, as a rule, the judge should decide as based on the reason which shall compensate the damage of the injured party better⁶⁸¹. However, if the law or the injured party demanded the application of the other liability cause, then the judge decides accordingly⁶⁸². It should be underlined that basing the claims on the breach of obligation is more beneficial for the injured⁶⁸³. This is because it is in favor of the injured party when the provisions related to the proof of the fault, the liability of the employer and the statute of limitation are based on the breach of obligation⁶⁸⁴.

breach of obligation shall not always constitute tort and accordingly it shall not give rise to the compensation obligation. Tekinay, Akman, Burcuoğlu and Altop, p. 641.

⁶⁸⁰ Hatemi, p. 69; Oğuzman and Öz, Vol. II, p. 292.

⁶⁸¹ However, basing on a legal reason in some issues and basing on another legal reason in other issues is not allowed. All the provisions of the legal reason, which is used against the offender, should be applied only. Oğuzman and Öz, Vol. II, p. 293.

⁶⁸² Ayözger, p. 307.

⁶⁸³ Safa Reisoğlu, *Türk Borçlar Hukuku Genel Hükümler*, 23.Edition (İstanbul: Beta Yayınları, 2012), p.391; Hatemi and Gökyayla, p. 294. However, in case of concurrent causes, it should not be derived that always the provisions of contractual liability shall be applied. See: Supreme Court, 3.CC., D.24.12.2001, M. 2001/10432, R. 2001/10922. - Legalbank Elektronik Hukuk Bankası, (Access Date: 12.02.2019).

⁶⁸⁴ Reisoğlu, p. 391.

The first difference between the liability due to the breach of obligation and the tort liability is the proof of fault. In compliance with the art. 112 of the TCO, the debtor cannot be relieved of the liability unless he/she proves that no liability can be imposed due to the activities that constitute a breach of obligation⁶⁸⁵. However, in tort liability, the injured party is required to prove that the damage is caused by the fault of the damaging party in compliance with the art. 50 of the TCO⁶⁸⁶. As can be understood from these provisions, if the damages caused as a result of unlawful processing of the personal data by the data controller are based on both reasons, then the data subject should prefer the breach of obligation relation since the liability for the breach of obligation shall be more favorable with respect to the proof of the fault. Another difference between two reasons of liability is the statute of limitation. According to the art. 146 of the TCO, while the statute of limitation is ten years as of the occurrence of the damage in the contractual relation, this term is two years in tort liability starting from the date on which the injured party becomes aware of the damage and the identity of the person liable for the compensation, and in any case, ten years starting from the date on which the activity is performed. The provisions of breach of obligation are more favorable since the term for the statute of limitation is longer according to the provisions of the breach of obligation.

Another important difference between these two liabilities is about the liability of the employer or the performance assistant. In case a person processes the personal data on behalf of the data controller as based on a legal relation and such processing damages the other party of the legal relation then application of the provisions of breach of obligation is more advantageous for the injured party. If tort relation is to be applied due to an activity performed by a third party, then the data controller shall be liable within the scope of the employer's liability. In employer's liability, which is a state of strict liability, the data controller can be relieved of this liability by bringing the evidence of salvation⁶⁸⁷. However, if this is based on contractual liability, then hostility

⁶⁸⁵ Eren, p. 1061.

⁶⁸⁶ In other words, while the burden of proof in tort belongs to the injured party, the debtor is required to prove that he is not faulty in the liability arising of the breach of obligation. Hatemi and Gökyayla, p. 295.

⁶⁸⁷ Accordingly, the data controller shall be relieved of the liability if he/she pays due care and attention while selecting the employee, giving instructions with respect to the work, supervising and inspecting,

can be directed to the damaging party due to the damages caused to the counterparty of the contract by the person acting as the performance assistant. In other words, the data controller, who is a party of the contract, shall be liable in person for the activity of the performance assistant which constitutes a breach of obligation. He/she cannot be relieved of liability by bringing evidence of salvation⁶⁸⁸. Accordingly, even if the data controller employs performance assistant, then he/she shall be responsible personally for the activities of the performance assistant which constitute a breach of obligation, if there is a relation of obligation between the data controller and the data subject. This way, the data subject can demand the compensation of the damage arising of the breach of obligation, from the data controller who is generally stronger in economic terms.

CONCLUSION

Mankind have puzzled his brain trying to solve the unknown phenomena and events from the first ages of the history up to today's modern society. In order to achieve this, he tried to access information and aimed to transfer such information to the next generations to make it permanent. Accordingly, the uncertain, indefinite issues that require solution became certain, net and understandable. Information is the most important tool to satisfy the curiosity of the man. Various instruments, means and methods are formed in order to satisfy this feeling. In the first ages of the history, mankind, drawing pictures on the walls of the caves, using fire in order to transfer information to each other and to the next generations, invented writing which is the fundamental and the most important instrument for the transfer of information. Since

which are required in order to prevent the occurrence of the damage. In this case, the damaging party can demand the compensation of the damage from the employee only as based on the fault of the employee. Tandoğan, p. 450.

⁶⁸⁸ Tandoğan, p. 446.

then, many inventions, which the people of that era could not even imagine of, were made and today's information society is reached.

Mankind was not only curious about the information concerning the phenomena and events, he was also curious about the information about each other. The state administrators collected information about the people living in the country in order to provide for their needs, to offer better service or to strengthen his own authority. Individuals need information about the other people when determining the person to marry, when the employers select the employees and when the businessmen meet the needs of the customers.

Today, accessing information was facilitated extremely with the development of the technology. Both the development of the internet and inclusion of artificial intelligence in our lives, resulted in collection of our personal data continuously and enabled classification and categorization of such gigantic information. This causes individuals to encounter violations of the protection of private life, the right of self-determination, freedom of expression and many more fundamental rights and freedoms. Individuals feeling that his/her data are collected without his/her consent shall not feel themselves free in that society and shall not be able to direct their preferences by their own wills. This shall make that society an open-air prison, in a sense. This is because the financiers of the capitalist order acquire the information related to the individuals and we evolve towards a world in which the individuals are not only the users of the products, but the personal data are also a product themselves. This condition, although indirectly, shall commoditize the individuals and the behaviors or habits, which we make or which we think that we choose, shall be made within the direction of the purposes of the person or people who have acquired data concerning us. This shall make the individual a slave, thinking he is free, but is directed by those who have the power.

The right for protection of the personal data is important for this reason. The right for protection of the personal data enables the individuals to establish dominance over the information concerning such individuals. Thanks to this right, the data subjects shall be informed of the people processing their data, shall be able to prevent the processing of the data, to learn whether his/her personal data are processed or not, to learn whether

these are transferred to the third parties or not or if transferred, to whom these are transferred and to demand the deletion, updating or correction of the personal data processed.

In our country, the issue of the protection of the personal data was started to be discussed both in the business world and the law societies following the entry into force of the LPPD in 2016 and foundation of the Personal Data Protection Authority and the awareness in the society was raised considerably. Punishment were started to be applied to the data controllers by the Authority due to unlawful processing of the personal data and these decisions were published over the website. Likewise, many decisions for conviction were given by the penal courts as a result of unlawful recording, acquisition or spread of the personal data which is regulated as a crime in our Penal Code. Also in our Constitution, protection of the personal data is regulated as a fundamental right. Due to this reason, the issue of the protection of personal data in the Constitution, Penal and Administrative law branches became an issue of arguments in the doctrine.

Protection of the personal data in the field of Civil Law is considered within the scope of the protection of the personal rights. Before the LPPD took effect, the protection of the personal data of the data subjects was considered by the civil legists within the frame of the personal values and the protection was regulated by the art. 23, 24 and 25 of the TCC. However, as the LPPD took effect, the boundaries concerning were drawn for the states which are considered to be the lawful for the processing of the personal data, the rights of the data subject and the obligations of the data controller were defined in a clearer manner. The legal liability of the data controller is examined in this study since we noticed that there is no detailed study in Turkish law about how the damage of the data subject, specifically as a result of unlawful data processing by the data controller, shall be compensated. The following conclusions are drawn within the scope of this study;

- 1- Within the scope of the provisions of the LPPD, only the natural persons are protected. This is because only the information about the natural persons are expressed in the definitions concerning the personal data. Generally natural persons are protected in the data protection regulations of the European Union

and some major international institutions. However, the legal persons are also included within the scope of the protection of personal data in the regulations concerning some sectors and in some Northern European countries. Inclusion of only the natural persons within the scope of the LPPD does not mean that the damages of the legal persons arising of the unlawful processing of the data cannot be claimed from the data controller. The legal persons can file an action for compensation against the data controller with respect to the damages suffered as a result of unlawful processing of their data which should be protected within the frame of trade secrets. The most important difference here is the nature of the data of the legal persons is not public and the owner of such data desires them to remain confidential. However, the nature of the data of the natural persons is broader. If the data of the natural persons, which are not related to the privacy of a person and even are made public, are processed unlawfully this shall constitute an attack to the personal rights.

- 2- Today, the personal data of especially the children become public with the development of technology and the data which are processed at small ages follow them throughout their lives. Due to this reason, the protection of the personal data of the minors is specifically significant. The issue of protection of the personal data of the minors which is regulated by separate provisions in GDPR is not regulated in the LPPD. The personal data of the children are protected by the general data protection provisions regulated for everyone. GDPR regulates that the personal data of the children of 16 years of age or older can be processed by their consent, in cases where consent is applicable. It is stated that the personal data of the children under 16 years of age can be processed with the consent or approval of their parents. Since there is no provision in the LPPD, general provisions shall apply for giving the consent. If it is assumed that the children have the power of discernment for the mentioned processing activity, the consent given shall be accepted to be valid and the personal data processed shall be lawful. This is because the processing of the data is a right that is tightly associated to the person for the minor.
- 3- There is no provision in the LPPD concerning the protection of the personal data of the deceased people. On the other hand, in GDPR the data of the

deceased people are not within the scope of the Regulation. According to Turkish law, the personal data of the deceased person should be protected within the scope of the arguments related to the protection of the personal values, against unlawful processing activities such as acquisition, collection, storage or transfer. In our opinion, the personal data which are the personal values of the deceased person should be protected according to the opinion in German law related to the protection of the personal values following death. This is because the person's belief that his/her personal data shall not be unlawfully processed following his/her death is included in the free development of the personality. Due to this reason, the relatives or the inheritors of the deceased person can protect the person's rights.

- 4- There is no provision in the LPPD and GDPR with respect to the protection of the personal data of the unborn child. Accordingly, the unborn child should be protected in compliance with the general provisions as a result of processing the personal data. Accordingly, under appropriate conditions, the unborn child can file actions for material and moral compensation for the damages to occur as a result of unlawful processing of the personal data at the very moment he/she enters mother's womb (as fetus) provided that he/she is born alive. Moreover, all the data of the unborn child shall also be considered as the personal data of the mother also. Due to this reason, even if the child is not born in full or alive, the mother can demand the protection of the mentioned data within the frame of the LPPD.
- 5- Genetic and biometric data are considered as personal data of special nature both in the LPPD and GDPR. Due to this, they are protected more strictly. However, while both the genetic and biometric data are considered to be personal data of special nature in LPPD regardless of the processing purpose, the genetic and biometric data processed for determination of the data subject's identity only are considered as personal data of special nature in GDPR. In our opinion, the genetic and biometric data processed in order to determine the identity of a natural person should be considered as personal data of special nature. Otherwise, the scope of the personal data of special nature would be very broad and this may cause major problems in practice.

- 6- Determination of the legal nature of the personal data is important in order to determine which legal regime to apply during the protection of the personal data.

There are three dominant opinions, as the personal rights, property rights and intellectual property rights, in the doctrine concerning which legal benefit such protection of the personal data serves. In our study, we believe that it is required to protect the personal data within the frame of the personal rights which is the dominant opinion in Europe and Turkey. Today, the protection of the personal data is not considered only within the scope of the protection of private life. In addition to this, it is considered as a separate right which covers the right for development of the personality freely, human dignity, freedom of belief and freedom of thought. Accordingly, the purpose of the protection of the fundamental rights and freedoms of the individuals is significant. This state is underlined both in the LPPD and GDPR. Moreover, free and correct flow of the information in addition to this protection shall be enabled more conveniently thanks to such regulations.

- 7- When the personal data of the data subject are processed within the scope of the activities of a legal person, the data controller liable for such processing is not the natural person processing such personal data, but it is the legal person itself. The cases where the Law required the otherwise or the cases where the legal person clearly indicates the data controller without any doubt shall constitute the exceptions of this state. The person acting on behalf of the legal person shall be liable for the damages to occur as a result of the processing activity only if such person processed such personal data unlawfully with the means of the legal person but out of such legal person's control and field of activity. For the continuity of the civil law liability of the data controller, it is required that the conditions of the employer's liability or the performance assistant's liability are created. However, if the required technical and administrative measures within the scope of LPPD are not taken, then he/she shall have strict liability.
- 8- The liability of the data controller due to the unlawful processing of the personal data occurs in three ways. These are the tort liability of the data

controller, liability due to the breach of obligation and culpa in contrahendo liability. Each personal data processed, which are not based on any legal relation or without any pre-contractual negotiations, causes tort liability. In this case, art. 23-24 and 25 of the TCC, which protect the personal rights, can be applied. If the data subject suffers any damage due to such processing, then he/she can file an action for compensation in compliance with the art. 25 of the TCC and art. 49 and 58 of the TCO.

- 9- For the data controller to be liable for tort, first the personal data processing activity should be unlawful or the data security should not be provided. A damage should be suffered due to this and there should be a causal relationship between this damage and the unlawful activity. Finally, in cases where fault is sought, the data controller is required to be faulty.
- 10- Since the attacks made to the personal values shall be considered as unlawful as a rule, processing of the personal data is unlawful as a rule. However, these shall become lawful if the lawfulness conditions stated in the articles 5 and 6 of the LPPD exist. Moreover, the data controller is required to act in compliance with the general principles stated in the 4th article even if such conditions exist. The burden of proof that the personal data are processed lawfully belongs to the data controller. Accordingly, the data controller can be relieved of the liability by proving the existence of one of the lawfulness reasons, against the data subject claiming that his/her personal data are processed unlawfully.
- 11- One of the lawful reasons for processing the personal data is the explicit consent of the data subject. It should be underlined here that the explicit consent regulated in the LPPD and the consent regulated in the art. 24/2 of the TCC are different concepts, although they do not conflict with each other. Both types of consent are the reasons for lawfulness. However, stricter conditions are required for the explicit consent to be valid. Although the conditions of the consent regulated by the art. 24/2 of the TCC also apply for the explicit consent, there are some other conditions in the explicit consent such as the declaration of will by the data subject.

- 12- The issue of whether the fault of the data controller shall be sought or not in unlawful processing of the personal data is important. Although there is an provision concerning the liability of the data controller and the data processor in the art. 82 of the GDPR, lack of such a provision in the LPPD is a flaw. In GDPR, it is stated that the data controller is required to prove that he/she is not liable in any manner whatsoever for the event causing the damage, in order to be relieved of the liability. This means the data controller cannot be relieved of the liability by proving that he is not faulty. However, LPPD only refers to the general provisions with respect to the legal liability of the data controller. Since the rule is the fault liability and the exception is strict liability in the general provisions, in our opinion, the data controller is required to be faulty in order to be liable. However, the fault of the data controller is not sought, in the event of some cases of strict liability regulated by the law. Moreover, the data controller also has strict liability for the activities of the data processor in compliance with the art. 12/2 of the LPPD. Within the scope of this issue, it should be discussed whether or not the data controller has strict liability according to the provisions of the risk liability. It would have been appropriate if LPPD contained an explicit regulation in order to avoid such discussions.
- 13- For the data controller to be liable due to the breach of obligation, there should be a valid contractual relation between the data controller and the data subject. This contract is required to impose primary and secondary obligations on the data controller and the data controller is required to act contrary to such obligations. Moreover, material or moral damage should as a result of the breach of obligation and there should be an appropriate causal relationship between this damage and the activity which breaches the obligation. In the liability for the breach of obligation, the fault shall be sought, as in the tort liability. Moreover, the burden of proof is reversed in compliance with the art. 112 of the TCO and the data controller is required to prove that he/she is not faulty in order to be relieved of the liability for the breach of obligation.
- 14- An action for compensation and an action for fulfillment can be filed together, when the obligation of the processing and security of the personal data is considered within the scope of the performance obligation. However, only an

action for material or moral compensation can be filed in order to remedy only the damage suffered in cases where this is in the nature of secondary obligation for assisting or protecting the fulfillment.

- 15- According to the provision of the art.15/1 of the TCC, the parties can decide that they shall not be liable for the slight faults, with an contract to be concluded beforehand. There are no provisions in the LPPD that prohibit the conclusion of a non-liability agreement between the data controller and the data subject with respect to the activity of processing the personal data. However, according to the principles in the LPPD related to the processing of the personal data, it can be construed that the data controller shall even be liable for the slight negligence, when the lawfulness reasons and the obligations of the data controller are taken into account. Since these provisions regulated by the law are mandatory provisions, non-liability agreements to be concluded by the parties should be definitely invalid.
- 16- During the contractual negotiations, the parties are required to act in compliance with the rules of bona fides and observe the benefits of each other. During such negotiations, the damaging party causing the damages due to his/her faulty activities is held liable in compliance with the provisions of CIC. Due to this reason, CIC liability shall apply in case of unlawful processing of the personal data or non-deletion due to the disappearance of the processing reason, even if a contract is not formed between the data controller and the data subject.
- 17- Usually the data subject suffers moral damage as a result of unlawful processing of the personal data. In cases where the personal data are processed unlawfully, this shall constitute an attack on the personal values of the data subject such as his/her private life, honor and dignity, development of the personality freely and freedom of thought. Moreover, since a reference is made to the general provisions by the art. 14/§ of the LPPD, the action for compensation is filed in compliance with the provisions of the art. 58 of the TCO and the art. 25 of the TCC. Although the provision of the art. 58 of the

TCO is regulated among the tort provisions, it is also applied for the cases of breach of obligation in compliance with the art. 114/2 of the TCO.

- 18- A moral damage should be suffered in order to decide for moral compensation. However, there is no full agreement with respect to the definition of the moral damage in the doctrine. According to the objective opinion, while moral damage is a reduction in the personal values of an individual, it is the pain, suffering and grief felt as a result of such reduction in the personal values of an individual according to the subjective opinion. Mixed opinion on the other hand, takes both into consideration and argues that the moral damage has two factors. And in some cases, it even considers the reduction only in the personal values, within the scope of the moral damage. According to this opinion, which we also agree, processing of the personal data only as unlawfully is not sufficient for the occurrence of the moral damage. The mentioned unlawful processing should also have moral and psychological negative impacts on the data subject, as well.
- 19- For the data subject to file an action for compensation against the data controller for the unlawful processing of the personal data, he/she should have the capacity to sue. Accordingly, the data subjects with full capacity have the capacity to file any and all types of actions. If the data subject has partial disability, then he/she can file action for protection of the personal rights and action for moral compensation, without the permission of his/her legal representative since these are rights which are tightly associated with the personal rights. On the other hand, the permission or the consent of the legal representative is required in order to file an action for material compensation. The legal representatives of those with absolute disability can file any and all types of cases on behalf of them.
- 20- The joint and several liability of several persons due to the same data processing activity may occur under various circumstances. This state may occur as a result of unlawful data processing by the joint data controllers or as a result of the performance of the data processing activity by the data processor on behalf of the data controller. Or, joint and several liability occurs if the

personal data are processed unlawfully by the employee in cases where the data controller is the employer.

- 21- Joint data controller become jointly and severally liable in compliance with the art. 61 of the TCO due to causing the same damage jointly. This is regulated by the art. 82/2 of the GDPR and it is stated that each data controller involved in the processing activity shall be liable for all the damage to occur. Accordingly, the data subject can claim the whole damage from each data controller, regardless of the degree of their effect on the damage and the part of the damage such effect influences.
- 22- The data controller shall have the strict liability for the unlawful activities of the data processor processing the personal data on behalf of the data controller. In the art. 12/2 of the LPPD, it is stated that the data controller shall jointly liable with the data processor for the unlawful processing of the personal data in case the personal data are processed by another natural or legal person on behalf of the data controller. due to this reason, the data subject can directly file an action for compensation against the data processor as well as the data controller for the remedy of the damage.
- 23- In case the personal data are unlawfully processed during the work assigned to the employee by the data controller, then the data controller shall have strict liability as the employer. The provision of the art. 66 of the TCO imposes on the employer, the obligation to pay due attention and care during the instructions given to the employees connected to him/her. Presumptively it is assumed that the data controller have acted contrary to the duty of care with respect to the damages which the employees gave to a third party. Accordingly, the data controller is relieved of liability if he/she proves that attention and care required in order to prevent the damage was shown when selecting the employee, giving instructions for the work, supervising and inspecting. The data controller's duty of care is specifically regulated in the art. 14/3 of the LPPD. Accordingly, *"The data controller shall be obliged to conduct necessary inspections, or have them conducted in his own institution or organization, with the aim of implementing the provisions of this Law"*. While

the data controller, as the employer, is liable in compliance with the provisions of strict liability, the employee shall be liable directly in compliance with the provisions of tort. Due to this reason, there shall be liability for the same damage for different reasons, which is a type of joint and several liability.

24- Unlawful recording, acquisition, providing or transfer of the personal data are the typical activities that constitute a crime within the scope of the TPC. Due to this reason, the actions for compensation to be filed with respect to such activities according to the art. 72/2 of the TCO shall be subject to the statute of limitation of the penal actions. In compliance with the art. 66 of the TPC, the term for the statute of limitation for the penal actions is 8 years in offenses requiring punishment of imprisonment or punitive fine not more than five years. Since the statute of limitation is shorter than 10 years in penal actions, the effect of the statute of limitation of 10 years provided by the art. 72/1 of the TCO shall continue to apply. However, the shorter statute of limitation which is 2 years shall be effective following the expiry of the statute of limitation of the penal action. In addition, since the statute of limitation for the penal action is 15 years where the crime of processing personal data is a major crime, the term for the statute of limitation for filing an action for compensation shall also be 15 years as of the date on which tort is committed.

If non-performance of the obligations arising of a legal relation is realized as unlawful processing of the personal data or not providing the data security, this state shall usually constitute an attack to the personal rights and as a result, the tort liability and the contractual liability shall compete. In such cases, the judge should base the decision on the reason of liability which shall be more beneficial for the injured party. However, if the data subject demands otherwise or on which legal liability to base such decision is specifically stated in the law, then the judge is required to comply with these.

BIBLIOGRAPHY

Ackoff, Russel. (1999). From Data to Wisdom. *Ackoff's Best*, John Wiley& Sons. pp. 170-172.

Akgül, Aydın. (2014). *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. İstanbul: Beta Basım Yayın.

Akıncı, Ayşe Nur. (2017). AB Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi. *Çalışma Raporu-6*. Ankara: T.C. Kalkınma Bakanlığı.

Akıncı, Şahin. (2017). *Borçlar Hukuku Bilgisi Genel Hükümler*. (10.Edition) Konya: Sayram Yayınları.

Akkanat, Halil. (2004). *Ölümün Özel Hukuk İlişkilerine Etkisi*. İstanbul: Filiz Kitabevi.

Aksoy, Hüseyin Can. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*. Ankara: Çakmak Yayınları.

Alsenoy, Brendan Van. (2016). Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 7 (3), 271-288.

Andrade, Norberto. (2011). Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. *IFIP Advances in Information and Communication Technology*, 352, 90-107.

Antalya, Osman Gökhan. (2018). *Borçlar Hukuku Genel Hükümler*. Vol. I (Vol. I), (2.Edition) İstanbul: Legal Kitabevi.

Antalya, OsmanGökhan. (2018). *Borçlar Hukuku Genel Hükümler*. Vol. II (Vol. II=, (2.Edition) İstanbul: Legal Kitabevi.

Antalya, Osman Gökhan. (2017). *Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukuna Manevi Tazminatın İki Aşamalı Olarak Hesaplanmasına İlişkin Model Önerisi (Manevi Zararın Belirlenmesi)*. İstanbul: Legal Yayınları.

Arıdemir, Arzu Genç. (2008). *Sözleşmeye Aykırılıktan Doğan Manevi Tazminat*. İstanbul: Onikilevha Yayıncılık.

Arslan, A. İsmet. (1980). "Ceza Hukuku Kurallarının Haksız Fiilden Doğan Tazminat Taleplerine Etkisi (I)". *Yargıtay Dergisi*. 6(1-2), 157-178.

Atlan, Hülya. (2015). *Manevi Zararı Tazmin Yolları*. İstanbul: Onikilevha Yayıncılık.

Ayözger, Çiğdem. (2019). *Kişisel Verilerin Korunması-Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*. (2. Edition) İstanbul: Beta Yayınları.

Başalp, Nilgün. (2011). *Sorumsuzluk Anlaşmaları*. İstanbul: Onikilevha Yayıncılık.

Başalp, Nilgün. (2004). *Kişisel Verilerin Korunması ve Saklanması*. Ankara: Yetkin.

Baysal, Başak. (2012). *Zarar Görenin Kusuru-(Müterafik Kusur)*. İstanbul: Onikilevha Yayıncılık.

Berber, Leyla Keser. (2014). *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması*. İstanbul: Onikilevha Yayıncılık.

- Beytar, Erbil. (2017). *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*. İstanbul: Onikilevha Yayıncılık.
- Bilge, Mehmet Emin. (2005). *Ticari Sırların Korunması*. Ankara: Asil Yayıncılık.
- Braun, Cihan Avcı. (2018). Kişisel Verilerin İşlenmesinde Rıza. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*. 15 (1), 13-33.
- Cansel, Erol/ Özel, Çağlar. (2017). *Borçlar Hukuku Genel Hükümler*, Vol. I, (2. Edition) Ankara: Seçkin Yayıncılık.
- Çekin, Mesut Serdar. (2018). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*. İstanbul: Onikilevha Yayıncılık.
- Çekin, Mesut Serdar. (2016). *6098 Sayılı Türk Borçlar Kanunu Madde 71 Çerçevesinde Tehlike Sorumluluğu*. İstanbul: Onikilevha Yayıncılık.
- Demircioğlu, Huriye Reyhan. (2009). *Güven Esası Uyarınca Sözleşme Görüşmelerindeki Kusurlu Davranıştan Doğan Sorumluluk*. Ankara: Yetkin Yayınları.
- Dural, Mustafa / Ögüz, Tufan. (2018). *Türk Özel Hukuku-Kişiler Hukuku*. Vol. II. İstanbul: Filiz Kitabevi.
- Dülger, Murat Volkan. (2019). *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi.
- Erdem, Mehmet. (2010). *Özel Hukukta Zamanaşımı*. İstanbul: Onikilevha Yayıncılık.
- Eren, Fikret. (2018). *Borçlar Hukuku Genel Hükümler*. (23. Edition) Ankara: Yetkin Yayınları.
- Forde, Aidan. (2016). The Conceptual Relationship Between Privacy and Data Protection. *Cambridge Law Review*, 135, 135-149.
- Gezder, Ümit. (2017). *İçerik Sağlayıcının ve Yer Sağlayıcının Hukuki Sorumluluğu ve Sorumluluk Muafiyeti*. İstanbul: Beta Yayınları.
- Gezder, Ümit. (2014). *Türk Medeni Hukuku-(Başlangıç-Kişiler-Aile Hukuku)*, İstanbul: Beta.

Gezder, Ümit. (2010). *Türk- İsviçre Hukukunda Culpa in Contrahendo Sorumluluğu*. Ankara: Beta Yayınları.

Gezder, Ümit. (2007). Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliği Koruma Teorisi, *İÜHFİM*, 65 (1), 207-222.

Gönen, Doruk. (2011). *Tüzel Kişilerde Kişilik Hakkı ve Korunması*. İstanbul: Onikilevha Yayıncılık.

Gürpınar, Damla. (2017). Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk, *D.E.Ü. Hukuk Fakültesi Dergisi*, Prof. Dr. Şeref Ertuş'a Armağan, 19, 679-694.

Gürsel, İlke. (2016). *İşçinin Kişisel Verilerinin Korunması Hakkı*. İstanbul: Adalet Yayınevi.

Gürsoy, Kemal Tahir. (1973). Manevi Zarar ve Tazmini. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 30 (1), 7-56.

Hatemi, Hüseyin. (2017). *Kişiler Hukuku*. (6. Edition) İstanbul: Onikilevha Yayıncılık.

Hatemi, Hatemi / Gökyayla, Emre. (2017). *Borçlar Hukuku Genel Bölüm*. (4.Edition) İstanbul: Vedat Kitapçılık.

Hatemi, Hüseyin / Oğuztürk, Burcu Kalkan. (2014). *Kişiler Hukuku*. İstanbul: Vedat Kitapçılık.

Helvacı, Serap. (2017). *Gerçek Kişiler*. (8. Edition) İstanbul: Legal Yayınları.

Helvacı, Serap. (2001). *Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar*. İstanbul: Beta Yayınları.

İnal, Emrehan / Baysal, Başak. (2008). *Reklam Hukuku ve Uygulaması*. İstanbul: Onikilevha Yayıncılık.

İnal, Emrehan. (2005). *E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması*. İstanbul: Vedat Kitapçılık.

İşevi, A. Semih / Çelme, Burçin. (2005). Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak. *Bilgi Dünyası Dergisi*, 5 (2), 1-16.

- Kaneti, Selim. (2007). *Haksız Fiilde Hukuka Aykırılık Unsuru*. İstanbul: Kazancı Hukuk Yayınları.
- Kapancı, Kadir Berk. (2016). Ceza Mahkemesi Kararlarının Hukuk Mahkemesi Kararlarına Etkisi. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 7, pp. 511-552.
- Kaya, Mine. (2015). *Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması*. Ankara: Seçkin Yayınları.
- Kaya, Cemil. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas Kişisel Veriler ve İşlenmesi. *İÜHFM*, 69 (1-2), 317-334.
- Kayıhan, Şaban/ Ünlütepe, Mustafa. (2018). *Borçlar Hukuku Genel Hükümler*. (6. Edition) Ankara: Seçkin Yayıncılık.
- Kılıçarslan, Seda Kara. (2017). *Adam Çalıştırmanın Sorumluluğu*, Ankara: Turhan Kitabevi.
- Kılıçoğlu, Ahmet. (2018). *Sınai Haklarla Karşılaştırmalı Fikri Haklar*. (4.Edition) Ankara: Turhan Kitabevi.
- Kılıçoğlu, Ahmet. (2017). *Borçlar Hukuku: Genel Hükümler*. (21. Edition) Ankara: Turhan Kitabevi.
- Kılıçoğlu, Ahmet. (1973). Haksız Fiillerden Sorumlulukta Ceza Hukuku İle Medeni Hukuk İlişkisi. *AÜHFD*, 29 (3), 185-225.
- Kılıçoğlu, Kumru. (2012). *Yansıma Yoluyla Zarar*. Ankara: Turhan Kitabevi.
- Kocayusufpaşaoğlu, Necip. (1980). Kişilik Haklarını Koruyan Manevi Tazminat Davasına İlişkin Yeni Gelişmeler. *Sorumluluk Hukukunda Yeni Gelişmeler I. Sempozyumu*, Ankara, 21-22 Ekim 1977, İstanbul: Fakülteler Matbaası.
- Korff, Douwe. (1998). Practical Implication of the new EU General Data Protection Regulation for EU and non-EU Companies. *Final Report*, Cambridge: Commission of the European Communities.
- Korkusuz, Mehmet Refik / Korkusuz, Mustafa Halit. (2018). *Hukuk Başlangıcı*. (4.Edition) İstanbul: Beta Yayınları.

Kutlu, Önder / Kahraman, Selçuk. (2017). Türkiye’de Kişisel Verilerin Korunması Politikasının Analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5 (4), 45-62.

Küzeci, Elif. (2018). *Kişisel Verilerin Korunması*. (2. Edition) İstanbul: Turhan Yayıncılık

Livingstone, Sonia / Carr, John/ Byrne, Jasmina. (2015). One in Three: Internet Governance and Children’s Rights. *Global Commission on Internet Governance, No: 22*.

Livingstone, Sonia / Haddon, Leslie / Görzig, Anke / Ólafsson, Kjartan. (2011). Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 Year Olds and Their Parents in 25 Countries. *EU Kids Online, Deliverable D4. EU Kids Online Network*. London.

Macenaite, Milda. (2017). From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation. *New Media and Society*, 19 (5), 765-779.

Macenaite, Milda / Kosta, Eleni. (2017). Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?. *Information & Communications Technology Law*, 16 (2), 146-197.

Nomer, Haluk Nami. (2015). *Borçlar Hukuku Genel Hükümler*. (Reviewed 14. Edition) İstanbul: Beta Yayınları.

Oğuzman, M. Kemal / Barlas, Nami. (2018). *Medeni Hukuk Giriş, Kaynaklar, Temel Kavramlar*. (24.Edition) İstanbul: Vedat Kitapçılık.

Oğuzman, M. Kemal / Öz, Turgut. (2018). *Borçlar Hukuku Genel Hükümler*. Vol. I. (16.Edition) İstanbul: Vedat Kitapçılık.

Oğuzman, M. Kemal / Öz, Turgut. (2018). *Borçlar Hukuku Genel Hükümler*. Vol. II. (16.Edition) İstanbul: Vedat Kitapçılık.

Oğuzman, M. Kemal / Seliçi, Özer / Oktay-Özdemir, Saibe. (2018). *Kişiler Hukuku- Gerçek ve Tüzel Kişiler*. (17. Edition) İstanbul: Filiz Kitabevi.

Özbudun, Ergun. (2014). *Türk Anayasa Hukuku*. (15. Edition) Ankara: Yetkin Yayınları.

Özdemir, Hayrunnisa. (2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara: Seçkin Yayınları.

Özel, Sibel. (2004). *Uluslararası Alanda Medya ve İnternette Kişilik Haklarının Korunması*. Ankara: Seçkin Yayınları.

Öztan, Bilge. (2000). *Şahsın Hukuku Hakiki Şahıslar*. (9. Edition) Ankara: Turhan Kitabevi

Gutwirth, Serge / Hert, Paul De (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. in E. Claes, A Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/ Oxford, Intersentia, 61-104.

Pearce, Henry. (2017). Big Data and the Reform of the European Data Protection Framework: An Overview of Potential Concerns Associated with Proposals for Risk Management-based Approaches to the Concept of Personal Data. *Information & Communications Technology Law*, 16 (3),

Petek, Hasan. (2015). *Kişilik Değerlerinin Ölümünden Sonra Korunması*. Ankara: Yetkin Yayınları.

Reisoğlu, Safa. (2012). *Türk Borçlar Hukuku Genel Hükümler*. (23.Edition) İstanbul: Beta Yayınları.

Samuelson, Pamela. (1999). "Privacy As Intellectual Property?". *Stanford Law Review*, 52 (5), 1-42.

Saraç, Senem. (2013). *Türk Borçlar Kanunu'nda Tehlike Sorumluluğu*. İstanbul: Onikilevha Yayıncılık.

Serozan, Rona. (2017). *Medeni Hukuk, Genel Bölüm/ Kişiler Hukuku*. İstanbul: Vedat Kitapçılık.

Serozan, Rona. (1990). Manevi Tazminat İstemine Değişik Bir Yaklaşım, Prof. Dr. Haluk Tandoğan'ın Hatırasına Armağan. *Banka ve Ticaret Hukuku Araştırmaları Dergisi*, 67-101.

Sözüer, Eren. (2017). *Unutulma Hakkı- İnsan Hakları Hukuku Perspektifinden Bir İnceleme*. İstanbul: Onikilevha Yayıncılık.

Sulu, Muhammed. (2016). *Ticari Sırların korunması*. İstanbul: Onikilevha Yayınları.

Suluk, Cahit / Karasu, Rauf / Nal, Temel. (2018). *Fikri Mülkiyet Hukuku*. (2.Edition) Ankara: Seçkin Yayıncılık.

Şahin, Osman. (2011). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması. *Bilgi Teknolojileri ve İletişim Kurumu*. Ankara.

Şimşek, Oğuz. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*, Ankara: Beta.

Tandoğan, Haluk. (2010). *Türk Mes'uliyet Hukuku*. (Exact Copy of 1961 First Edition) İstanbul: Vedat Kitapçılık.

Taştan, Furkan Güven. (2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: Onikilevha Yayıncılık.

Tekinalp, Ünal. (2005). *Fikri Mülkiyet Hukuku*. İstanbul: Vedat Kitapçılık

Tekinay, Selahattin Sulhi / Akman, Sermet / Burcuoğlu, Haluk / Altop, Atilla. *Borçlar Hukuku*. (Reviewed and Expanded 6. Edition) İstanbul.

Tezcan, Durmuş. (1991). Bilgisayar Karşısında Özel Hayatın Korunması. *Anayasa Yargısı*, 8, 385-392.

Ünal, Yenal. (2009). "Bilgi Toplumunun Tarihçesi". *Tarih Okulu Dergisi*, 5, 123-144.

Ünver, Tülay Aydın. (2011). *Ceninin Hukuki Konumu*. İstanbul: Onikilevha Yayıncılık.

Walden, Ian / Sawage, Nigel. (1988). Data Protection and Privacy Laws: Should Organisations be Protected?. *International and Comparative Law Quarterly*, 37 (2), 337-347.

Yıldırım, Abdulkerim. (2018). *Türk Borçlar Hukuku Genel Hükümler*. (7.Edition) Ankara: Monopol Yayınları.

Yıldız, Esra Tekil. (2003). İnternet Üzerinde Kişisel Verilerin Korunması. *Prof. Dr. Fahiman Tekil'in Anısına Armağan*, İstanbul, 791-793.

Yılmaz, Sabire Sanem. (2018). Kişisel Verilerin Korunması Regülasyonu ve Unutulma Hakkı. *İstanbul Barosu Dergisi*. 92 (5), 188- 193.

Yılmaz, Malik. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49 (1), 95-118.

Yücedağ, Nafiye. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri. *İÜHFİM*, 75 (2), 765-789.

Reports and Guidelines

Article 29 Data Protection Working Party. (2013). *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies*. Brussels.

Article 29 Data Protection Working Party. (2013). *Opinion 03/ 2013 on purpose limitation*. Brussels.

Article 29 Data Protection Working Party. (2011). *Opinion 15/2011 on the Definition of Consent*. Brussels.

Article 29 Data Protection Working Party. (2010). *Opinion 1/2010 on the Concepts of "Controller" and "Processors"*. Brussels.

Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the Concept of Personal Data*. Brussels.

Article 29 Data Protection Working Party. (2005). *Working document on data protection issues related to RFID technology*. Brussels.

European Data Protection Supervisor. (2012). *Opinion of the European Data Protection Supervisor on The Data Protection Reform Package*. Brussels.

European Data Protection Supervisor. (2011). *A comprehensive approach on personal data protection in the European Union*. Brussels.

Personal Data Protection Authority. (2017). *6698 Sayılı Kanunda Yer Alan Temel Kavramlar*. Ankara.

Personal Data Protection Authority. (2017). *Veri Sorumlusu ve Veri İşleyen*. Ankara.

Personal Data Protection Authority. (2017). *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*. Ankara.

Personal Data Protection Authority. (2017). *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*. Ankara.

Personal Data Protection Authority. (2017). *Kişisel Verilerin İşlenme Şartları*. Ankara.

Personal Data Protection Authority. (2017). *Açık Rıza*. Ankara.

Special EUROBAROMETER 359. (2011). *Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels: European Commission.

The United Kingdom Information Commissioner's Office (ICO). (2016). *Overview of General Data Protection Regulation*. London.

Internet Sources

Cimpanu, Catalin. (2019). *DailyMotion Discloses Credential Stuffing Attack*. ZDNet. <https://www.zdnet.com/article/dailymotion-discloses-credential-stuffing-attack/> (Access Date: 15.03.2019).

Cohen, Simon. (2019). Kanopy Privacy Breach Reveals Which Movies Members Have Been Streaming. Digital Trends. <https://www.digitaltrends.com/home-theater/kanopy-streaming-data-breach/> (Access Date: 24.03.2019).

Cranium, Are Genetic Data of Unborn Children Subject to Data Protection Under the GDPR, <https://www.cranium.eu/genetic-data-unborn-children-subject-data-protection-gdpr/> (Access Date: 13.02.2019)

Fendoğlu, Hasan Tahsin. (2014). "2001 Anayasa Değişikliği Bağlamında Temel Hak ve Özgürlüklerin Sınırlanması (13th Article of the Constitution)". *Elektronik Sosyal Bilimler Dergisi*, Vol.I, <http://dergipark.ulakbim.gov.tr/esosder/article/view/5000067866> (Access Date: 16.02.2019)

Leskin, Paige. “The 21 Scariest Data Breaches of 2018”, *Business Insider*, 30.12.2018; <https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#3-exactis-340-million-19> (Access Date: 23.02.2019).

Newman, Lily Hay. “Facebook Stored Millions of Passwords in Plaintext- Change Yours Now”, *Wired*, 21.03.2019, <https://www.wired.com/story/facebook-passwords-plaintext-change-yours/> (Access Date: 24.03.2019).

Tutesigensi, Melissa. “Theology Lecturer Breaches Confidentiality in Mass Email”, *Palatinate*, 25.01.2019, <https://www.palatiniate.org.uk/theology-lecturer-breaches-confidentiality-in-mass-email/> (Access Date: 22.03.2019).

Türk Dil Kurumu, *Güncel Türkçe Sözlük*, <http://sozluk.gov.tr/?search-input=veri> (Access Date:11.04. 2018)

Türk Dil Kurumu, *Güncel Türkçe Sözlük*, <http://sozluk.gov.tr/?search-input=veri> (Access Date:11.04.2018)

Türk Dil Kurumu, *Güncel Türkçe Sözlük*, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c753d5730b0a0.29668248 (Access Date: 07.09.2018).

Whittaker, Zack. “A family tracking app was leaking real-time location data”, *TechCrunch*, 23.03.2019, <https://techcrunch.com/2019/03/23/family-tracking-location-leak/> (Access Date: 24.03.2019)