

THE EFFECTS OF THE LAW ON THE PROTECTION OF PERSONAL DATA ON HUMAN RESOURCES APPLICATIONS OF LOGISTICS COMPANIES

Ayşe İLAGA ÇAKIR¹

Abstract

Today, private and government agencies collect many personal data about individuals every day. Personal data; means any kind of information about the person whose identity is specific or identifiable. Technology has evolved to allow individuals and institutions to share and disseminate information worldwide. Personal Data Protection is a right of individuals that need to be protected against unauthorized use of their data by other individuals or organizations. This right has been taken under protection by amendment of Article 20 of the Constitution. In addition, amendments were made to some other laws and finally, on 24 March 2016, the Law No. 6698 on the Protection of Personal Data was adopted in the Turkish Grand National Assembly. The law, regulates the procedures and principles to be followed by the obligations of natural and legal persons, and imposes important provisions on all companies that process, carry or store personal data. One of the sectors affected by the law is logistics. In this study, the national and international legal regulations and the Law No. 6698 which are related to the protection of personal data were examined. In the logistics sector, the effects of this law on human resources practices, difficulties, causes and consequences were investigated with a screening approach and in-depth interview methods. In the sector, a study on this subject has not been found, in this respect it is thought that it will contribute to the literature and the sector.

Keywords: Logistics Human Resources, Personal Data, Processing of Personal Data, Right to Protection of Personal Data,

JEL Classification: K10, K31, L91, O15

KİŞİSEL VERİLERİN KORUNMASI YASASININ LOJİSTİK ŞİRKETLERİN İNSAN KAYNAKLARI UYGULAMALARINA ETKİLERİ

Öz

Günümüzde, özel ve devlet kurumları, hergün bireyler hakkında birçok kişisel veri toplamaktadır. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Teknoloji, kişi ve kurumların bilgiyi paylaşması ve dünya çapında yaymasına izin verecek şekilde gelişmiştir. Kişisel verilerin korunması, bireylerin verilerinin başka kişi veya kuruluşlar tarafından yetkisiz kullanımına karşı sahip oldukları bir haktır. Bu hak, başta Anayasamızın 20. Maddesinde değişiklik yapılarak koruma altına alınmıştır. Ayrıca diğer bazı yasalarda değişiklikler yapılmış ve son olarak 24 Mart 2016 tarihinde, Kişisel Verilerin Korunması Kanunu TBMM Genel Kurulu'nda kabul edilmiştir. Kanun, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemekte, kişisel veri işleyen, taşıyan veya saklayan firmalar için önemli hükümler getirmektedir. Yasadan etkilenen sektörlerden birisi de lojistikdir. Bu çalışmada, kişisel verilerin korunması hakkındaki ulusal ve uluslararası yasal düzenlemeler ve 6698 sayılı yasa incelenmiştir. Yasanın, lojistik şirketlerin insan kaynakları uygulamalarına etkileri, zorlukları, sebep ve sonuçları tarama yaklaşımı ve derinlemesine görüşme yöntemleri ile araştırılmıştır. Sektörde bu konuda yapılan bir çalışmaya rastlanmamıştır, bu açıdan literatüre ve sektöre katkı sağlayacağı düşünülmektedir.

¹ Ayşe İlaga Çakır, Maltepe University, PhD In Logistics And Supply Chain Management, Istanbul, Turkey, av.aysecakir@gmail.com ORCID: 0000-0003-1291-7564.

Anahtar Kelimeler: Lojistik İnsan Kaynakları, Kişisel Veri, Kişisel Verilerin İşlenmesi, Kişisel Verilerin Korunması Hakkı.

JEL Sınıflaması: K10, K31, L91, O15

1. Introduction

The logistics sector in the world and in our country is growing with each passing day, and its importance is understood better. Logistics, which has been perceived only as “transportation” until recently, has emerged as an integrated sector with the basic stages such as procurement, production, storage, transport, and packaging, and many components such as business development processes, customer service, and information technologies.

Developments in the logistics sector have also affected the labor force of the sector. It has supported the increase in the competitive environment, the development of companies, and innovations. Human resources and technology are very important for the sector. Numerous companies operate in the Turkish logistics sector. A large number of people are employed together with the sub-sectors. Due to the size of the operational dimension of logistics activities, the number of field workers is considerably higher than the number of office workers, and there is a high labor turnover (Jobnak Human Resources, 2010).

In today's rapidly developing and competitive world, human resources departments are very important for businesses. Activities such as providing human resources, organization, and supervision are carried out by human resources. Human resources are also very important in the labor-intensive logistics sector, where personnel circulation is high and there are different business areas. Therefore, these departments are required to have the knowledge and preparation to adapt to dynamic, technical, social, and legal changes (Gelincik, n.d.).

Human resources departments interview many candidates and receive job applications. Each interview and application is data sharing, and these data are also stored after recruitment. As the worker starts to work, data sharing continues with workplace rules and practices. Personal data recording is often carried out in different areas of our lives. It is possible that these data can be obtained, used, and misused by unauthorized persons, so it is important to protect the data. It is a right granted to individuals to demand the protection of data.

This right is protected by international conventions to which we are a party, the Constitution, and laws. In this context, Law No. 6698 on the Protection of Personal Data was adopted in the Turkish Grand National Assembly on 24 March 2016. The law regulates the obligations and procedures and principles of the natural and legal persons who process, carry, or store personal data. The imposition of hefty fines and imprisonment is regulated for individuals and institutions that violate the rules. The law is also closely related to logistics companies, where the human factor is very important, which employ workers in different fields, have a high labor turnover, and process a large amount of personal data.

The study consists of 7 sections. After the introduction section, in the second section, the concept of personal data and its brief history and legal regulations are explained, and in the third section, literature research is explained. In the fourth section, the method of study is explained, and in the fifth section, the human resources applications of the companies operating in the logistics sector are explained.

In the sixth section, the requirements for human resources within the scope of the Law on the Protection of Personal Data, responsibilities of employers, sanctions, board decisions, and regulations are explained, and in the last section, conclusions and suggestions are stated.

2. Concept Of Personal Data, Its History, And Legal Regulations

Personal data is defined in Law No. 6698 on the Protection of Personal Data (LPPD) as “All the information relating to an identified or identifiable natural person” (Law No 6698 , 2016). In this case, the information that defines the identity of persons such as name, surname, date of birth, place of birth, as well as the data that identifies the cultural, physical, economic, social or psychological identity of persons and the data that will make persons identifiable such as identity, social security number, and telephone number are all personal data. Furthermore, CV, picture, image and audio recordings, fingerprint, genetic information of persons are also personal data. Some of your personal data is further protected. This group is defined as sensitive (private) data (Carey, 2009, p. 81).

The legal regulations on the protection of personal data have taken their current form by passing through various stages.

Table 1. Historical Process of The Protection of Personal Data (Kaya & Taştan, 2018)

Institution	Document	Year
United Nations	Universal Declaration of Human Rights	1948
EU Council	European Convention on Human Rights	1950
United Nations	International Covenant on Civil and Political Rights	1966
Organization for Economic Cooperation and Development (OECD)	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	1980
EU Council	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention No. 108)	1981
United Nations	Guidelines for the Regulation of Computerized Personal Data Files	1990
EU Commission	Data Protection Directive (95/46/EC)	1995
EU Council	Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Additional Protocol No. 181)	2001
EU Commission	Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002/58/EC)	2002

Institution	Document	Year
EU	European Union General Data Protection Regulation 2016/679 (GDPR)	2016
EU Council	Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108+)	2018

Developments in information technologies from the second half of the 20th century to the present day have become more evident nowadays, affecting not only business processes but also all areas of life. The logistics sector is also an area where these developments are felt strongly.

Rapid digitalization has brought about the need for new regulations in the legal field. The digitalization of information with increasing speed and the need to re-establish the impaired imbalance against the individual have made it necessary to determine the rules of law to which data processing processes will be subject. In this respect, the law on the protection of personal data is closely related to digitalization.

As a matter of fact, the first regulations for the protection of personal data were adopted in the years when computers and databases began to process information about individuals on a large scale. Nowadays, more than one hundred and twenty states have legal regulations in this field.

International conventions, constitutions, and laws form the basis of the regulations for the protection of personal data. Furthermore, secondary regulations such as bylaws, regulations, and communiqués issued in order to demonstrate the application of laws are located in the legislation.

2.1. International Regulations

- A.** One of the international regulations on the protection of personal data to which our country is a party is the Council of Europe Convention No. 108. This Convention introduces regulations within the framework of the EU standards for the protection of personal data. The Convention entered into force in 2016 in our country.
- B.** In addition to this convention, “Additional Protocol No. 181 regarding supervisory authorities and transborder data flows” was prepared and entered into force in 2016 in our country.
- C.** Convention no. 108 was amended in 2018 and entered into force in the EU as 108+.
- D.** The European Union General Data Protection Regulation was published in 2016. Although it is a regulation that has entered into force in EU countries, under certain conditions, it also includes sanctions for companies operating in non-EU countries. This is an important regulation that logistics companies that have business relations with the EU member states should take into consideration.

E. The International Labor Organization was established as a United Nations specialized organization. It is working to improve social justice and workers' rights internationally.

At the 1996 Committee of Experts meeting, the Code of Practice on the Protection of Personal Data of Workers and recommendations on this matter were adopted.

F. The Council of Europe adopted recommendations on the protection of personal data, setting out principles to be applied in various sectors such as employment, medical data banks, scientific research and statistics, direct marketing, social security, insurance, police records, electronic payment, telecommunications, and the internet. It is observed that the subject of "Employment" is included in the recommendations. In our country, these recommendations were taken into consideration during the preparation stage of LPPD no. 6698. It is stated that these principles will be included in the regulations to be made regarding different sectors. In the meantime, the decisions of the Personal Data Protection Board on various sectors and matters started to be formed.

2.2. National Regulations

A. The Constitution of the Republic of Turkey is one of the leading national regulations on the protection of personal data. In Article 20 of the Constitution titled the right of privacy (Additional paragraph: 7/5/2010-5982/2 art.), it is stated that "Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law." (Constitution of the Republic of Turkey , 1982, p. art.20). This article accepts the protection of the personal data of all citizens as a right and forms the basis of all other legal regulations.

B. The important legal regulation that forms the basis of the study is Law No. 6698 on the Protection of Personal Data. Article 1 of the Law is as follows: "The purpose of this Law is to protect fundamental rights and freedoms of people, particularly the right to privacy, with respect to processing of personal data and to set forth obligations, principles and procedures which shall be binding upon natural or legal persons who process personal data."

Paragraph 5/1 of the Law stipulates that "personal data cannot be processed without the explicit consent of the data subject," and the following paragraph 2 provides exceptions. The processing of personal data of special nature is regulated in paragraphs 6/1-2 of the Law, which state that "(1) Personal data relating 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 are deemed to be personal data of special nature." "(2) It is prohibited to process the personal data of special nature without explicit consent of the data subject." Exceptions in some cases concerning explicit consent are also provided in paragraph 3 of the same article.

There are basic principles that must be followed in all cases in which personal data is processed. These principles are regulated in Article 4/2 of the law: "a- Lawfulness and conformity with rules of bona fides, b- Accuracy and being up to date, where necessary, c-

Being processed for specific, explicit and legitimate purposes, ç- Being relevant with, limited to and proportionate to the purposes for which they are processed and d- Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.” It is compulsory to comply with these principles under all conditions and circumstances. This means that, All transactions that process the personal data must comply with these principles. Example: Digital filing, big data, etc.

In Article 3 of the law, it is stated that “d) Personal data: all the information relating to an identified or identifiable natural person, e) Processing of personal data: 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.” For example, it is an obligation to act in accordance with the principles set forth in the law, not only when a particular person's address is recorded, but also erased.

In Article 7 of the law, it is stated that “(1) Despite being processed under the provisions of this Law and other 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.” “(3) Procedures and principles for the erasure, destruction or anonymizing of personal data shall be laid down through a by-law.” The regulations concerning the application procedure are included in the ongoing articles of the law. The regulation mentioned in the article entered into force by being published in the Official Gazette on 28 October 2017. Furthermore, the Communiqué on Procedures and Principles for Data Controller Applications was published in the Official Gazette on 10 March 2018 (Law No 6698 , 2016).

- C. As can be seen, in the law, data protection provisions are regulated in detail. The regulations of protection of personal data are also included in Articles 135-140 of Turkish Criminal Code No. 5237, and penal sanctions are indicated in case of non-compliance. In addition, people whose rights have been violated have the right to compensation.

3. Literature Review

The protection of personal data is an important issue that has been taken under protection by legal regulations in many countries in recent years. For this reason, studies in the literature have increased. The studies conducted in various fields and subjects related to the protection of personal data are given in Table 2.

Table 2. Literature Review (Kartal, 2018, pp. 1-18)

Author	Year	Country	Content
Ketizmen and Ülküderner	2007	Turkey	Protection of Personal Data in E-Government Applications
Kaya	2011	Turkey	Sensitive (Personal) Data and Its Processing in the Context of the European Union Data Protection Directive

Author	Year	Country	Content
Saadet	2012	Turkey	Regulations for restricting the confidentiality of communication
Barnard-Wills et al.	2016	EU Countries	An effect of data protection reforms on cooperation between EU institutions
Turan	2016	Turkey	Duties and responsibilities of data controller institutions, compliance with legislation, attention and care
Chua et al.	2017	Malaysia	Compliance of public and private institutions with personal data protection principles.
Hoel and Chen	2017	Norway	Data protection and privacy.
Tikkinen-Piri et al.	2017	EU countries	EU General Data Protection Regulation: changes and their effects on personal data collection companies
Erbaş	2017	Turkey	Observation of Workers in the Electronic Environment within the Scope of Law No. 6698 on Protection of Personal Data
Dülger	2016	Turkey	Operability of systems for the protection of personal data.
Kartal	2018	Turkey	Protection of Personal Data: A Conceptual Assessment on the Turkish Banking Sector
Avcıoğlu	2018	Turkey	Right to protection of personal data in Turkish law
Oğuz	2018	Turkey	General principles of the law on the protection of personal data

According to the literature review, it is observed that various studies have been carried out on the protection of personal data. However, in the field of the logistics sector, no studies have been found on the protection of personal data in human resources applications. In this respect, it is thought that the study will contribute to the literature and the sector.

4. Method

The methodological orientation of the study is qualitative. Data on the subject to be examined were collected from a homogeneous group (logistics companies) using the screening approach and exploratory method. Screening research is one of the most appropriate methods for social scientists to collect and describe natural information. Screening research can be used for exploration, description, and explanation purposes. First of all, official, statistical, sectoral and case resources, Personal Data Protection Board decisions, and administrative arrangements were used. During the in-depth interviews conducted with the human resources authorities of the logistics companies operating in Istanbul, information was collected about the applications of the protection of personal data, difficulties encountered, reasons, effects and suggestions, and information was collected about other logistics company applications by examining examples from official resources. Finally, all this information was evaluated, and suggestions were made.

5. Logistics Company Human Resources Applications

Since the Law on Protection of Personal Data is a law covering all fields of public and private sectors, it is important that all workers and employers learn, implement, and adapt the law to business processes. The law has determined the period of registration of businesses in the system. Administrative sanctions of the legal regulations awaiting the owners of the enterprises have been regulated if Registry of Data Controllers registration is not done. Compensation and criminal cases may also be subject according to the nature of the concrete event.

The provisions of the law are of a general nature and apply to all personal data described in the law. Since the subject of the study is the protection of personal data in human resources applications in the logistics sector, in this section of the study, the applications in the doctrine and the effects of the law on the enforcement bodies are explained. Human resources interviews of the companies were also conducted within this scope.

In-depth interviews were conducted face-to-face with the human resources officers of the logistics companies where the appointment was made. Information was collected about the applications of the law in the sector, the difficulties, and demands. Moreover, official websites of many logistics companies were examined, and information and documents on the implementation of the law were obtained. The companies interviewed are based in Istanbul and have been operating in the logistics field for nearly 30 years in different business lines (automotive, textile, etc.) nationally and internationally. As can be understood from the history of companies and the extensiveness of their fields of activity, many workers are employed in the field and office environment. Therefore, there are numerous regulations and applications on the subject. Since the companies demand to keep their names confidential, the name of the company cannot be shared. Prior to the appointment, resources were reviewed on the protection of personal data, doctrine applications, legal regulations were investigated, the data collected were analyzed, and then the companies were interviewed with the questions determined. During the meeting, information was obtained not only on the questions determined but also about the new questions and the practices and the effects of the law according to the course of the applications.

5.1. Personal Data Collection, Information, Consent, and Application

The processing of personal data starts from the application to the job advertisements of the businesses as candidates. With the forms created by the employer (company's human resources department), candidates are asked to answer various questions. In addition, apart from the form information, candidates are required to submit (by hand or on a digital platform) exam documents, tests, diplomas, certificates, health reports, etc., and the processing of personal data is continued through applications such as obtaining information about the candidate from third parties, application of tests, monitoring with cameras and tracking devices.

This process continues with the recruitment of the selected candidates, the continuation of the employment and even the termination of the employment contracts, or the storage of the information of the applicants who have not been recruited. Therefore, even if the contract is terminated and the candidate is not selected; the obligation to protect, store, erase, destroy, anonymize and not to transfer all personal data collected by the employer, continues. However, there may still be situations in which the personal data of the worker may be at risk. In fact, applications such as recording the time that the worker goes to the toilet monitoring how much he/she moves with the device placed in his/her chair, and prohibiting the use of special-purpose phones and/or computers even during breaks can be applied in many workplaces (Uncular, 2018). Likewise, during the study, the statements of workers working in logistics warehouses, *"450 workers work in the warehouse part of our workplace. We work with a four-shift system... We go to toilets with a card."*, were reached in an interview on the working conditions. This is an example of the recording of the times of workers' visits to the toilet (Doğan, 2017).

As mentioned, the first meeting of human resources with candidates starts with applications to the job advertisements. The interviewed companies were asked primarily about the content of the questions asked to candidates in the applications to the job advertisements, the method by which the information is received (via the internet, during the interview, etc.). The companies stated that they started an archive review with the enactment of the law and that resumes and attached documents from job/worker search websites and those protected within the company are reviewed, but the processes will take a long time to complete. Within the scope of the studies, they stated that application forms were renewed and the questions asked to candidates were revised and brought into compliance with the law. Furthermore, one of the companies stated that they have given information regarding to the LPPD to the workers who had started to work before the law unpublished and they had signed information documents containing consent texts and that the application would continue in this way for those to be recruited.

All of the companies stated that, according to the law, they put general information text on their official websites under the title of "Protection of personal data and privacy policy." They also stated that for recruitment human resources applications, they would add a section to the job applications section of the web pages that they allowed the processing of data with the information text so that candidates could read and be informed before the application. As explained in the statutory section of the study, data processors do not return personal data they receive and will need to obtain the explicit consent of the candidate if they wish to store it. In accordance with the mandatory provision of the law, it is important that candidates are provided with clear information and their explicit consent is received when obtaining personal data (exceptions are specified in the law).

Nowadays, with the development of science and technology, applications such as monitoring of workers with electronic and biometric access control systems, listening to their phones, monitoring of their e-mails, internet accesses, social media accounts, tracking of their vehicles with GPS, observation of their behaviors in the workplace have become widespread and easier. In accordance with Article 3/3 of the International Labor Organization (ILO) personal data application code, such applications are governed by the rules and principles of the data protection law (Uncular, 2018, p. 233).

A large number of drivers are employed in the transportation services of the logistics sector, and some information and documents are requested from both drivers and other candidates for their recruitment. In the information and documents obtained during the study, it was observed that job application forms/advertisements of many logistics companies include questions such as the name and profession of the candidate's spouse, the number of children, marital status, whether he/is disabled/ex-convict, membership in associations, retirement registration number, whether a lawsuit or investigation about him/her has been conducted.

However, questions asked to candidates about their family members, membership in associations, health-related questions that are not required by a job/duty definition and questions such as criminal record and former conviction should be limited to those important in terms of the job/duty definition (Uncular, 2018). Most of this information is Personal Data of Special Nature, which is defined in Article 6 of the law. The companies interviewed stated that they did not include such questions in their job advertisements and application forms, and revised their questions. In addition, they stated that they employ female workers in overseas branches as drivers and they do not include any statements that will make gender discrimination in job advertisements.

5.2. Personal Data Sharing, Application

The logistics sector is a sector that can employ workers in national and international fields. In this respect, it is also possible to transfer workers' personal data abroad. Article 9 of the Law sets out this issue in detail: *“(1) Personal data cannot be transferred abroad without the explicit consent of the person concerned”* Exemptions are provided in the continuation of the article. It was asked to the companies, and they stated that they do not share personal data of workers between countries in their applications and that they provide foreign workers from the countries that they work (local workers). Furthermore, it was stated that the resume data are reviewed in the recruitment of the domestic personnel, that they do not share the candidate resumes recorded in their companies with other human resources or other group companies or persons without permission, that personal information about workers is not shared with the manager, colleagues, etc., and reference research is done with the approval of the worker. The obligations regarding data security are detailed in Article 12 of the law. Likewise, the Personal Data Protection Board made the following decision in the event that *“personal data processed during the job application process is unlawfully shared with other job applicants without any legal reason”*: *“That it is illegal to share personal data of a candidate applying for job among the data controllers under a group of companies without the explicit consent by using the same database and an administrative fine shall be imposed on said Company”* (Personal Data Protection Board, 2018).

5.3. Wearable Devices, GPS, Body Search, Health Data, and Application

With the development of technology, it is possible to monitor workers by tracking vehicles with GPS (The Global Positioning System). The opinion in the doctrine is that the employer is obliged to inform workers clearly that the tracking device is placed in the work vehicle (lorry, truck, etc.) and that the movements, driving, and position of the vehicle are recorded. It is stated placing this notification in each vehicle is the best way so that the driver can easily see it. The companies interviewed stated that their drivers sign an information document regarding the presence of GPS in their vehicles during their recruitment. Workers may be searched on the grounds that the entry of dangerous goods in warehouses or the unauthorized exit of valuable goods should be prevented. In the doctrine, it is argued that workers should be informed clearly, comprehensively, and extensively before such searches are done. Furthermore, it is possible to monitor places where workers work by a camera and to monitor their e-mails and searches on the internet. Decisions on this matter are state that the employer should clearly inform workers about the application. Some of the interviewed companies stated that with the publication of the law, procedures for these applications were determined by human resources, forms were prepared and signed by their workers during recruitment, and even included in employment contracts. Some stated that they were informed and they would revise their regulations in this way in accordance with the law.

Employers are increasingly using wearable devices to monitor, track, measure work speed, and breaks for workers' health and activities inside and outside the workplace. The data collected through sociometric name tags/badges are analyzed with artificial intelligence, and the productivity of workers is determined. These devices should be used without voice and conversation recording. Such devices are used in the logistics sector to direct warehouse employees to their next assignment. The misuse of these device applications will result in a breach of rights in the processing of personal data.

Health data is personal data of special nature. The results of the medical examination for the recruitment of the candidate / worker will only need to be indicated as to whether they are suitable for physical and / or mental recruitment (Uncular, 2018). Likewise, in the interviews with the companies, several companies stated that the application is made in this way, while others stated that as a result of the medical examination, the physician notifies whether the worker is suitable for the job and also sends a copy of the result to the personal file. Wearable devices can also be used to monitor the health of workers. Conducting such applications secretly without permission from the worker will be a breach of rights. Lastly, the companies were asked whether they receive any requests from candidates or workers regarding the erasure of personal data. The companies stated that they had not received any request on this subject and had not experienced such a situation yet.

The companies stated that when the law came into force, they organized workshops to be informed and to determine a road map. One of the companies stated that they had problems in the implementation of the regulation, that they could not understand the law, and that the fines envisaged in the law were disproportionate. In addition, they stated that infrastructure investment is required in order to carry out regulatory procedures, and it is appropriate that the relevant regulations and other regulatory procedures should be issued by the Personal Data Protection Authority as soon as possible. They further stated that the adaptation process should be extended, there is a lot of application and labor mobility especially in the logistics sector, the revision process of old and new data takes time, and they demand more time and solution.

6. Within The Scope Of The Lppd, The Responsibilities Of The Employer, Sanctions, The Requirements For Hr And The Personal Data Protection Board Decisions, Regulations

6.1. Employer's Responsibilities and Sanctions

Within the scope of Law on the Protection of Personal Data (LPPD), employers (human resources) have an obligation to inform candidates/workers as data controllers and to obtain their explicit consent. In addition, pursuant to Article 12 of the employer law, *“it is obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to a) prevent unlawful processing of personal data, b) prevent unlawful access to personal data, and c) ensure the retention of personal data.”* Employers cannot disclose the personal data of the worker/candidate to others in contradiction with the LPPD and cannot use it for any purpose other than processing. These obligations continue after the worker leaves the job.

Moreover, in accordance with Article 12/5 of the Law, *“In case the processed data are collected by other parties through unlawful methods, the controller shall notify the data subject and the Board within the shortest time.”* The company must register with the Data Controllers Registry. *“Natural or legal persons who process personal data shall be obliged to enrol in the Registry of Data Controllers before proceeding with data processing.”* (Law No 6698 , 2016).

As stated in the Application section, the law gives individuals (workers) the right to know if personal data has been processed, to request information if personal data has been processed, to know whether personal data has been used for its intended purpose, to know third parties to whom personal data has been transferred within the country or abroad, and to request the erasure or destruction of personal data, etc. Sanctions to be applied in case of violation were also determined (Belge, 2017).

When all of these issues are considered together, personal data requests should be suitable for the purpose of collection and not exceed this purpose, and a reasonable connection should be established between them for the purpose of collection. The worker should be clearly informed before collecting personal data. Employers must protect the data. The law imposes hefty fines and imprisonment on individuals and institutions that violate rights. The Personal Data Protection Authority is of great importance in ensuring compliance with the procedures and provisions of the law. The decision-making body of the authority is the Personal Data Protection Board. The Board is in the central position of the sanction system prescribed by law. In case of violations such as not complying with the obligation of registration and notification to the Data Controllers Registry and not fulfilling the decisions made by the Board, administrative fines ranging from 20.000 TL to 1.000.000 TL can be imposed (Law No 6698 , 2016, p. art.18).

Another regulation on this subject is the Turkish Criminal Code. In the articles 135-140 of the Law, recording of personal data, unlawfull sharing or seizing, realizing such situations in a qualified manner, infiltration into information systems, destroying data, etc. are included subjects. It is stated in the LPPD Law that the provisions of Turkish Criminal Code will be applied for crimes related to personal data. The punishment envisaged for regulated crimes is imprisonment (Law No 6698 , 2016) (Turkish Criminal Code , 2004).

Furthermore, in the event that data processing causes harm to the person concerned, private law sanctions and claims for damages may also be raised.

6.2. Requirements For The Employer (Human Resources)

The law concerns all public-private sectors, employers, and workers. Likewise, there are numerous rights violations through data sharing, not only by employers but also by workers. For example, there are “Board's principle decision dated 31/05/2018 and numbered 2018/63 concerning the processing of such data, outside the authority and purpose of the personnel authorized to access personal data before the data controller” and “Board’s decision on unlawful sharing of the personal data of special nature on the internet and social media channels” (Personal Data Protection Board, 2018) (Personal Data Protection Board, 2018). In this respect, it is important that all personnel, especially human resources enforcement bodies, receive training and have information about the legislation. Training can be as follows:

1. The first stage is that all company workers and managers receive training on the basic Law on the Protection of Personal Data legislation.
2. In addition, it is important that human resources workers receive Personal Data Protection information training for human resources management sub-processes after basic training. This stage may be in the subheadings of candidate applications, recruitment processes, worker-related processes, and former worker post-employment data.
3. The 3rd stage of the training is the Inventory training of Human Resources officers who have completed the 1st and 2nd training.
4. The final stage will be the documentation training, and it will be bringing the recruitment forms, employment contracts, workplace application forms, etc. into compliance with the law. According to the stages of the training, it will be beneficial to organize them with the participation of human resources officers, lawyers, quality officers, and IT experts.

In particular, Human Resources inventory studies will need to be revised in a digital environment. It is understood from the company interviews that most companies have difficulty in determining the road map to carry out these processes. *“In the decision of the dated 31/01/2018 PPD Board on the measures to be taken in the processing of personal data of special nature, providing regular training to employees, determining the personnel to be authorized to access the data, preserving and encrypting the data using cryptographic methods if the information is accessed electronically, and logging all transactions performed on the data securely, etc.”* were regulated in detail (Personal Data Protection Board, 2018).

6.3. Examples of The Personal Data Protection Board Decisions and Regulations

The Personal Data Protection Board decisions on personal data processing violations have started to be established. Some decisions are included in the relevant sections of the study. Regulations and communiqués are also issued. Some other board decisions and regulations are as follows:

Table 3. Personal Data Protection Board Decisions and Regulations (Personal Data Protection Authority, 2019)

Process	Subject
Board Decision	The decision that “the obligation of informing by the data controller and the need for explicit consent processes should be carried out separately”
Board Decision	“The Principle Decision on Protection of Personal Data in Service Areas such as Banks, Counters, Tables”
Board Decision	“The decision on the data controller that transfers health data to a third party without one of the processing conditions set out in Article 6 of the Law”
Regulation	The Communiqué on Procedures and Principles for Data Controller Applications
Board Decision	A Failure to Fulfill the Request for Erasure of the Personal Data of the Person Concerned
Regulation	The Communiqué on the Procedures and Principles to be Followed in the Fulfillment of the Obligation of Information
Regulation	The Regulation on Erasure, Destruction or Anonymizing of Personal Data
Regulation	Minimum elements to be included in the letter of undertaking to be prepared by data controllers for data transfer abroad
Regulation	The announcement of the Personal Data Protection Board dated 24.01.2019 on the principles and procedures for reporting personal data breaches

7. Conclusion And Suggestions

Due to the specific nature of the labor law, personal data are collected while the worker is still in the candidate stage. With the recruitment, an employment contract is drawn up, and the interaction between the personal data and the employer continues within the framework of the management authority of the employer and the dependence of the employee. The data remains at the employer when the employment contract is terminated. The Law on the Protection of Personal Data is a very important law for the human resources that process data since it defines “*the natural or legal person who processes personal data based on the authority given by the data controller on its behalf as the data processor.*” (Law No 6698 , 2016, p. art.3)

In the study, the specific nature of the labor law and the situation of the personal data protection applications in the logistics sector were examined. In the sector, workers' mobility is experienced intensively and rapidly. The number of field workers is higher than that of office workers, and many personal data entries are made every day.

There are different fields of work, and there is an international dimension of the works. Legal regulations are not limited to the rules of domestic law, but also include international conventions to which Turkey is a party. For all these reasons, it is important that international conventions and the Law on the Protection of Personal Data are taken into consideration by Human Resources officers of logistics companies and it is crucial that law harmonization studies are conducted in the time and manner ordered.

Sector Human Resources officers should first receive the Law on the Protection of Personal Data basic legislation training, LPPD information training for human resources sub-processes, the processes of recruitment, workers and those who leave should be determined, information technology infrastructure and business processes should be reviewed for data processing, protection, and storage, inventory preparation studies should be carried out, documentation training should be received, all personnel should be informed through the LPPD basic training, human resources forms and employment contracts should be revised in accordance with the law, informing and explicit consent texts should be prepared, and their placement on the digital media should be performed. While obtaining the consent of the worker, he/she should be fully informed and conscious about the subject he/she consents and should be informed by the employer. This provision is one of the most important regulations and forms the basis of correct data processing. In the literature, no study conducted on the subject of this research has been found.

It is thought that this study, which conceptually addresses the protection of personal data, includes national and international legal regulations and provides examples from applications, will contribute to the literature and the sector.

References

- Belge, A. (2017). Violations and Protection of Workers' Personal Data, in Particular Within the Framework of the Law on the Protection of Personal Data . *DEU Journal of Law Faculty*. C. 19, Special Issue (p. 1025-1051)
- Carey, P. (2009). Data Production. In Oxford, Data Protection: A Practical Guide to UK and EU Law (p. 81). Oxford University Press. Constitution of the Republic of Turkey, (1982) (No: 2709, p. art.20).
- Doğan, A. (2017, September 4). New address for irregular employment: Logistics warehouses. İstanbul: Evrensel. Retrieved from <https://www.evrensel.net/haber/331329/kuralsiz-calistirilmanin-yeni-adresi-lojistik-depolari>
- Gelincik, E. (n.d.). Human Resources and Quality Management in the Logistics Sector. Retrieved from International Transport and Logistics Service Producers Association: <https://www.utikad.org.tr/SektorelHaber.aspx?DataID=8645&Baslik>
- Jobnak Human Resources. (2010, December 23). Why are Human Resources Different in the Logistics Sector? Retrieved from <https://tr-tr.facebook.com/notes/jobnak-insan-kaynaklari>
- Kartal, M. (2018). Protection of Personal Data: A Conceptual Assessment of the Turkish Banking Sector . *International Journal of Economics and Innovation*, 4, (1-18)
- Kaya, M.B. & Taştan F.G. (2018), Personal Data Protection Law, On İki Levha Press. Law No 6698, (2016) Law on the Protection of Personal Data
- Personal Data Protection Board, (2018), Unlawful Sharing of Personal Data of Special Nature on Internet and Social Media Channels, Retrieved from <https://www.kvkk.gov.tr/3>
- Personal Data Protection Authority, (2019), Retrieved from <https://www.kvkk.gov.tr/5>

- Personel Data Protection Board, (2018), Unlawful Sharing of Personal Data Processed in the Job Application Process, Retrieved from <https://www.kvkk.gov.tr/> 1
- Personel Data Protection Board, (2018, May 31) Processing of such data outside the authority and purpose of the personnel authorized to access personal data before the data controller, (No:2018/63) Retrieved from <https://www.kvkk.gov.tr/> 2
- Personel Data Protection Board, (2018, May 31) Adequate Measures to be Taken by Data Controllers in the Processing of Personal Data of Special Nature, (No: 2018/10) Retrieved from <https://www.kvkk.gov.tr/> 4 Turkish Criminal Code (2004).
- Uncular, S. (2018). Protection of Workers Personal Data in Business Relationship. In Seçkin. Ankara. (p.186-187/233)