

# CONSEQUENCES AND THINGS TO DO REGARDING LAW ON PROTECTION OF PERSONAL DATA\*

Murat Volkan Dölger\*

Personal data, protection personal data, Personal Data Protection Act, and more generally, law on protection of personal data have become a popular and much debated field in Turkey in the last two years. For those involved in the matter, the interest dates back to earlier times; nevertheless, regardless of any involvement, everyone is somewhat familiar with the foregoing issues today.

Actually, there is no “uninvolved” section in the society within this field. As the content of concepts reveals, it is about “*persons*” and “*data of persons*”. Consequently, it is hard to talk about anyone not related with such problem. Today, as a result of significant daily use of information technologies and ensuring big data concept and artificial intelligence algorithms, everybody is a data controller, a data processor, or even a data subject. This is the reason behind the recent so-called “boom” of personal data protection.

It is worth noting that unawareness of certain persons about importance and relation of personal data protection does not necessarily mean this field is irrelevant for them. In this respect, one of the first things to do is to create sufficient and necessary awareness about the issue, in addition to and above theoretical information and discussions about personal data protection. First of all, individuals must be aware that personal data is something to be protected and understand why personal data requires protection. On the other hand, individuals should know they have to protect the personal data they process and the reason behind such requirement of protection. Therefore, the point for data subject person, data controller and data processor are to understand the essence of personal data protection. Once this essence is understood, it becomes possible to ensure that everyone acts in line with relevant legislation. Otherwise, personal data, like many other fields in Turkey, will be protected by legal norms but this protection will not be realized in practice.

This is why, talking about consequences of law on personal data protection, I think about researching and enhancing interest, knowledge and awareness level among individuals about law on personal data protection, rather than providing relevant legislation and theoretical information. For sure, this approach is not entirely independent of relevant legal regulations, and should be considered together with, above all, Personal Data Protection Law no. 6698. Indeed, personal data protection gained currency and became a point of debate in Turkey actually as of 7 April 2016, when Law no. 6698 came into effect. Accordingly, the primary objective of hereby study is to explain and tell about the atmosphere in Turkey about personal data protection since 7 April 2016, the misunderstood aspects of the problem, and the points to be improved.

## 1. Entry of Personal Data Protection Law no. 6698 into Force

In Turkey, personal data has begun to be talked and debated upon entry of Law no. 6698 into force. While other legislations comprised certain rules about the issue;, there was no legislation to

---

\* Hereby paper has been presented at “January 28<sup>th</sup>, Data Protection Day Conference” held by Personal Data Protection Authority in Ankara on 28 January 2019.

\* Phd., LL.M., Associate Professor of Criminal Law and IT Law / Lawyer

handle the problem as a whole. Such legislative absence led to many flaws and ambiguities in various fields including daily and economic activities; besides, it was considered as a huge defect in terms of EU harmonization process and commercial activities with Europe.

In this context, the Personal Data Protection Law, which came into effect on 7 April 2016, was established in order to eliminate the mentioned deficiency and to bring along regulations with regard to protection and processing of personal data. Accordingly, 7 April 2016 has to be considered as a defining and transforming point for Turkey in terms of personal data protection. Consequently, it is possible to assert that personal data protection has actually started in Turkey upon entry of Law no. 6698 into force and the inauguration of Personal Data Protection Board established pursuant to the Law.

## **2. Consequences of Law no. 6698**

### **a. Overview**

Today, we use personal data in almost all daily activities. During professional activities, we are data controller or data processor; when we are in the position of service receiver or consumer, we are data owner. Within a company, the human resources department keeps and records all personal data, including specific qualities of all employees or employee candidates. Hospital staff records the health data of the patients, bank employee keeps financial data of persons, while accountant processes financial data of persons. When we go to a place monitored by surveillance cameras and buy coffee with credit card, both our credit card details and images and voice are recorded and processed. The examples can be multiplied on the basis of all our daily activities. At this point, the following question should be asked: What are the rules according to which these data are collected and processed? Do persons, whose data are processed, have a right to speak? Law no. 6698 steps in at this stage and provides regulations as to all activities regarding personal data processing, including liabilities of data controller and data processor and the rights of data owner.

Upon entry of Law no. 6698 into force, the data controller should, above all, understand the following: *“As a data controller or processor, I cannot process personal data in the amount and manner I wish.”* Data subject, in turn, must be aware of the following: *“I am authorized on my data and have right to determine the future of my data; therefore, nobody can process my data without my explicit consent or without foreseen legal grounds.”* Indeed, Law no. 6698 establishes rules for each stage of personal data processing. Since these rules are explained in each article under the Law, I will not treat them here. Instead, I want to clarify the objective of the Law, in other words, to ensure awareness regarding essence of personal data protection.

Law essentially establishes general principles about processing of personal data, determines processing conditions for personal data, and regulates the rights of data subject. Thus, the conditions of data processing by data controller and data processor, and the possible relevant actions of data subject, are made clear. Data controller or data processor has to obtain explicit consent of relevant data subject or even to ground on one of processing conditions foreseen by Law, so as to be able to process personal data. At this stage, the explicit consent and the processing conditions foreseen by Law are worth noting. Prior to the Law, the conditions where personal data could be processed were regulated in other legislation depending on the situation; nevertheless, such conditions were significantly incomprehensive and restricted. On the other hand, they did not

comply with current approach on data protection law. Clear identification of conditions of personal data processing through the Law ensures presence of a general regulation about processing regardless of field or sector.

Besides, there was no prerequisite of explicit consent for processing the personal data of data subject. The concept of “explicit consent” entered our life with data protection law, and signifies the declaration of intent by data subject based on informing about personal data processing and declared in his free will. Data controller or data processor has to check whether the processing conditions foreseen by Law are in place in his activity, so as to be able to process personal data during an activity. If the conditions are met, he shall ground the activity of personal data processing on this condition; otherwise, he can process personal data only through explicit consent of data subject. Therefore, the groundless and purposeless data processing, which was common prior to the Law, is over.

As for data subject, he is granted authority on data in every sense. It is clarified that a person can give explicit consent for sharing and processing of data only without asserting any prerequisite and through his free will. Besides, the person is granted the right to learn the purpose and manner of data processing, as well as the persons to whom his data are transferred, and the opportunity to delete his data at his request. Thus, the person provided with the right to determine the future of his data as well<sup>1</sup>.

In fact, all the foregoing issues are collected under objectives and purposes of general principles regarding personal data processing. The characteristics and function of these principles are to identify the rules to be obeyed since the initial collection until any kind of processing of personal data. Accordingly, personal data can be processed only within the scope of general principles foreseen by legal regulations, pursuant to such procedures and principles. Therefore, these principles should be present in the essence of all personal data processing activities; likewise, all activities of personal data processing should be carried out in compliance with these principles. We will not indicate each of these principles herein; nevertheless, I would like to underline the fact that they are vital in order to comprehend the purpose and philosophy of rules regarding processing of personal data, or more generally, personal data protection<sup>2</sup>.

## **b. Audit mechanism**

Data protection authorities are foreseen by almost all national regulation on personal data protection, in order to check whether the requirements of these laws are met. One of the most important regulations under Law no. 6698 is an organ of regulation and supervision so as to fulfill the tasks given by the Law. For this purpose, Personal Data Protection Authority is founded and Personal Data Protection Board is inaugurated as essential decision-making body under the Authority.

Nevertheless, it will be unfair to consider the Board merely as an audit organ, even though it is principally treated as such. Since the Law came into effect, the Board issued and held directives, notifications, decisions and publications, studies and academic activities, proving it is much more

---

<sup>1</sup> For further information, see **Murat Volkan Dülger**, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi, İstanbul, 2019, p. 146-178.

<sup>2</sup> For further information, see **Dülger**, p. 107-146.

than an auditing body. Even though the sufficient public knowledge and awareness is yet to be established in terms of personal data protection, Board has played an important part in rendering personal data protection a popular issue even though Law no. 6698 came into effect only recently.

Indeed, the decisions made by the Board reveal this was the biggest change upon issuance of Law. Prior to the Law, there was no public body for data subject to direct an allegation of violation or complaint about processing of personal data; as for data controller, there was no risk or power of public body to carry out effective audit or adjudge on administrative fine in case he was subject to such violation allegation.

It is important for data subject to be duly informed and aware about his rights on personal data protection for optimum functioning of this mechanism. Even though there is no legal obligation in this regard, the Board actually carries out audit upon notification or complaint and takes decisions. Therefore, the realization of audit often depends on complaint by data subject.

Nevertheless, it should be remembered that the Law and Board are not foreseen for complaint by data subject and judgment by Board on punishment. Since the Law came into effect, data controllers unfortunately adopted an inaccurate approach, as if it were a Law established to punish them and the Authority were founded in order to fine. However, acts of data controller subject to violation regarding personal data processing underlie the complaint and violation allegation by data subject. Besides, it would be unfair to expect data controllers, who operated for long years without certain, clear and explicit legal rules about processing of personal data, to immediately and easily abide by the new circumstances; in fact, this is impossible. Establishment of legislation is one of the initial steps in order to ensure compliance of personal data processing with laws; nevertheless, this is far from being sufficient. All processes within a company do not become compliant with personal data processing legislation just because certain rules are established by law. Sufficient time and relevant effective process are required for this purpose. Indeed, in consideration of this fact, Board has not opted for administrative fine in some judgments even though violations were identified; instead, Board decided on “instruction” of data controller subject to violation. Accordingly, in addition to being an auditing mechanism, the Board and Authority both act as an organ that “regulates” this field which is new for Turkey; and this approach is very important.

Therefore, the Board, which is the auditing and decision mechanism in the field of personal data protection, should be considered as the greatest and most effective power in Turkey for establishment and improvement of personal data protection law in Turkey, thanks to its position and possibilities. As a matter of fact, the works and efforts by Board so far support this argument.

### **c. Compliance process**

Since its entry into force, the Law attracted interest from every sector and aroused attention particularly among major companies; this is primarily because of the “*compliance process*” postulated by the Law, as data controllers have to abide by it. Upon the Law, this process led to a somewhat panic among companies, which underwent a period of ambiguity and confusion regarding what to do.

Data controllers should act in compliance with principles, procedures and elements of data protection law at every stage regarding personal data as of its initial obtaining. This act in line with mentioned principles, procedures and elements depends on conduct of compliance projects called

*“process of compliance with Law”*. The objective of this process is to render all personal data kept and processed, including those available prior to effective date of Law, completely compliant with Law in both legal and technical terms at the end of the project. The process of compliance with Law covers a whole that consists of directives, notifications, resolutions, Board decisions, court practices, guidelines and exemplary practices based on the Law. At this stage, rather than providing information about how to conduct compliance process, I prefer talking about liabilities brought along by this process and how to handle them.

The first point to consider about compliance process is, unfortunately, the lack of understanding, the lack of wish of understanding or acknowledgement regarding the process. Moreover, there are data controllers who are “unaware” of the process. Companies, particularly those operating in international market, are bound by Directive 95/46/EC since 1995 and by GDPR since 25 May 2018; accordingly, they are already prepared and willing for compliance. As for domestic companies, they are yet to create necessary awareness about compliance process. On the other hand, I must indicate that relevant academic studies and efforts of the Board have provided great contribution in comparison to the situation at the time of entry of the Law into force; accordingly, the level of awareness is relatively higher about personal data protection. Nonetheless, the current level is far from the desired condition. In fact, while Turkey established Law no. 6698 in consideration of provisions under Directive accepted by European Union back in 1995, the EU states are subject to GDPR, which recently came into effect and which comprises much more actual and comprehensive provisions. Since the scope of GDPR is not limited with EU states, the companies operating in international market now have to act in compliance with GDPR provisions. Therefore, in the case of Turkey, the law on personal data protection should be improvement in order to ensure parallelism with EU directives and regulations.

Secondly, it is worth noting that data controllers tend to eliminate compliance process as an obligation and to refrain from it as much as possible. First of all, nobody can display any act harming the right of data subject to personal data protection during activity of personal data processing. All real and legal entities should act pursuant to the Law, or in more general sense, to law in all activities regarding personal data. Even though the certain groups are declared exempt from certain liabilities upon directives, notifications or Board decisions in the wake of the Law, the fundamental rule is that everyone should act in compliance with the Law and therefore conduct Law compliance projects.

On the other hand, the process evidently brings along an additional liability for data controllers. Since the process constitutes an uncertain field for data controllers and a long-lasting and tiresome task requiring participation of company employees, the data controllers refrain from its realization. At this stage, the process should not be considered as a project to be completed, but as a way to learn a human right, necessary for everybody in every aspect of life, and to ensure action in compliance with this right in every activity. Moreover, we should bear in mind that while we are data controller in a certain field, we are also data subjects in another, and want our rights to be respected as data subjects.

### **3. Process upon entry of Law into force: What changed in Turkey?**

First of all, a new legal branch, called law on personal data protection, is formed in Turkey. This branch is in such quality that it contacts with every other branch. Personal rights refer to civil law;

personal data protection right as a human right refers to constitutional law; offence upon violation of personal data protection refers to criminal law; personal data processing within the scope of corporate commercial activities refer to commercial law; processing of personal data in relation with shopping refers to consumer law; and administrative fines and regulations lead us to administrative law. Even more specific fields have a somewhat common point or contact with law on personal data protection. There is a huge traffic of personal data in all fields arising from IT media such as electronic communication, including e-commerce, e-sport, e-shopping, e-game etc. under IT law; this traffic brings along new regulations in parallel with provisions under law on personal data protection.

The foregoing examples can be extended to all legal branches. As I indicated above, personal data is ever-present where individual is present. Since law, in the most general and basic sense, is defined as integrity of rules organizing the society, personal data will be in question wherever law is in question; accordingly, law on personal data protection shall be present *a fortiori* in connection of with any legal branch.

Consequently, apart from formation of law on personal data protection, the other legal branches gained a new perspective in consideration of provisions about personal data protection. At this stage, my greatest expectation is that the law on personal data protection is not limited with relevant specific legislation and that necessary amendments are carried out on provisions within other laws about personal data protection in line with this perspective.

In my opinion, the awareness among law practitioners, theoreticians and society about personal data protection can be properly created if we try to instill it as a culture and not by considering it as a specific legal branch. Data protection law, within the scope of importance of personal data and the requirement for personal data protection, should be established in the entire society as a form of behavior and culture.

**Well, what should be done or has been done for this purpose? Have these efforts been useful?**

Is the legislation on personal data protection, which is established via Law no. 6698 and ensuing regulations, is sufficient to constitute the abovementioned approach? What is the actual situation?

First of all, Turkey is yet to attain sufficient level in the field of data protection law. This is not only because Turkey is backward in this context; it is also because a high level in terms of data protection law is required, given the position of Turkey. Indeed, Turkey is a country with high population; the majority of population uses IT tools in effective and intense manner; besides, commercial activities and relations are very intense on both national and international scale. These facts require an intense traffic of personal data processing. In such case, the requirement for personal data protection increases; as a result, the level of relevant protection and security should be very high in every aspect.

For sure, the requirement for personal data protection goes in parallel with difficulty of personal data protection. In other words, as the requirement for personal data protection goes higher, the personal data protection shall be as much difficult. Nevertheless, this cannot be an excuse in any manner whatsoever. The point here is significance of data protection law for Turkey and need for it; therefore, we have to adopt a policy of continuous development and improvement.

Since day one, the Law aroused great interest particularly for the companies have to comply with it and there is a relevant auditing mechanism. In this context, almost everyone tries to understand the liabilities brought by the Law and to abide by them. Legal advisors, who never worked on personal data or needed such effort within company before, were suddenly faced with the field of personal data protection. All law offices, regardless of whether they are specialized in private law, criminal law or commercial, began to receive questions from their clients with regard to personal data protection. For sure, there were legal experts who worked on personal data protection prior to effective date of the Law; nevertheless, everyone outside this tiny group began to wonder about personal data protection in an approach like, “*there is something called personal data*”. Therefore, I think that all of us, regardless of whether we worked about the matter prior to the Law, have been and are learning personal data within the scope of Law no. 6698 and personal data protection.

We should regard the situation through eyes of data controller or data processor and data subject. What did both parties learn upon the Law? What changed? On the part of data controllers, they obtained a perception that there is something called personal data and that they should protect it. Well, how? Does collaboration with legal experts conducting compliance projects and IT experts specialized in data security mean everything is duly done?

I have to state that Law compliance projects are compulsory but not sufficient on their own for ensuring conformity of a company to the Law; the projects merely constitute a portion of conformity to Law. It should be remembered that compliance process with a legal and technical team is only a project and that the parties set off to accomplish it. Nevertheless, processing of personal data is a continuous activity for each company. Evidently, compliance process does not mean that all data processing activities within a company are realized and completed during this project. The true objective is to lay a foundation where all personal data processing activities at any time from beginning to the end can be carried out in compliance with the Law, including personal data processing activities realized prior to Law. Therefore, compliance process should be considered not a project that begins and ends, but as an effort to lay a legal foundation for a continuous process. Such approach shall significantly facilitate conformity to law on personal data protection.

### **In order to adopt such perspective, what are the points to consider for data controllers?**

Thanks to IT tools, many activities can be realized without human action and digitalization increases in every sector. Nevertheless, we cannot talk about a data controller, for example, a company, which operates without human labor. Even though I foresee and believe this may be the case in near future, the current AI technology is not advanced enough yet. Therefore, in the case of companies, everybody in contact with the company, employees, should be taken into account; in other words, human factor should be taken into consideration. Given the fact that there are numerous employees in each department of a company, do all these employees have to be related with this process? For instance, can we consider legal consultancy department as an indispensable party in conduct of the process, and departments of sales and marketing, production or human resources totally out of the process? For sure, the project can be conducted in this way as well; but can such project serve the purpose foreseen by the Law?

As I said before, there is no legal branch or sector which is irrelevant to personal data; likewise, no department or unit within a company can be out of contact with personal data. Indeed, anybody

can be involved in data violation in deliberate or unintended manner, albeit the severity of such violation may depend on his respective position. Therefore, establishment of a ground in compliance with Law concerns everyone somehow operating within a company; it is a task for everyone. Accordingly, the most important point to consider for data controllers is training and awareness-raising among all persons employed or related with the company about data protection law. It is the first point to deal with. An employee should be told why the data controller has to protect personal data, rather than imposing pages of documents or legal norms and expecting him to obey them.

### **How can we ensure that a company employee comprehends the essence of data protection law?**

For sure, the first essential step is training about legislation and academic studies on data protection law, as well as practical questions and problems. In order to achieve the objective of such training, the second step is to organize regular trainings in certain intervals in consideration of relevant updates. These trainings must handle personal data protection as a respectable human right, and not in fear of sanction of administrative fine in case of violation or negligence.

At this stage, I want to touch upon frequent practical problems. Since the Law came into effect, we see that companies, particularly those which are or have conducted and accomplished compliance projects, have taken certain concrete steps. This is more apparent in areas where consumption is in question and one-to-one contact with humans is in common. In this respect, the most interesting point to me is to hang a frame of general information on personal data protection in almost every store or market, under various titles such as: *“Personal data protection”*, *“Our policy of personal data protection”* or *“Clarification on processing of personal data”*.

Are these texts necessary? In my opinion, they are. Nonetheless, such text will have no meaning or importance and can never attain the purpose unless the employees in such store or market are appropriately informed about personal data protection. Such text gains a meaning in case sufficient and capable data processors or employees are employed within data controllers. This is the approach to be adopted by data controllers with regard to law on personal data protection and related compliance processes. Otherwise, the compliance will be merely in appearance; however, we will have a powder barrel in the background. Therefore, the law on personal data protection should be put in contact with every person and point in a company from A to Z, rather than a general and rote-learning implementation. This is how it can become well-established.

### **Apart from data controller, which changes are observed with regard to data subject?**

In fact, data protection law is a whole; in other words, it is impossible to make a precise distinction about changes on the part of data controller and data subject. After all, the abovementioned liabilities on the part of data controller or data processor actually arise from data subject. More precisely, the liabilities of data controller shall constitute the rights of data subject, even though they do not completely match up with one another. Consequently, I have to indicate that all aforementioned issues also apply for data subject in the same manner. Besides, please remember that a person, who is in quality of data controller or processor during in fulfilling his professional activities, becomes a data subject as he purchases a product from a store; therefore, the concepts of data controller - data processor - data subject are often inseparable since these qualities may be

common in the same person.

On the other hand, personal data protection is essentially a right and this right is granted to data subject. The law on personal data protection grounds on protection and privacy of data subject. Accordingly, the purpose of Law no. 6698 is explained as protection of real entities whose personal data are processed and identification of liabilities and rules to be obeyed by those in charge of processing. Then, personal data protection law should be considered essentially as rights of data subject and liabilities of data controller or data processors.

As the Law came into effect and subsequent legal regulations were established, it became clear that personal data is a field to be protected and that this field should be protected by means of legal regulations. Therefore, the Law sets legal grounds for the right of individuals to personal data protection, and leads to emergence of the concept of data subject.

In fact, certain sections or groups, who now have many rights within the scope of personal data protection as data subjects, were not really aware of the situation. There was no sufficient awareness about why their data should be protected, which violations are committed on these data and for which purpose the data are used. Moreover, since violations on data and incidents such as commoditization of personal data by advertisement agencies were not in public sight, I think the lack of knowledge about the issue is not extraordinary. On the other hand, the entry of Law into force and the subsequent numerous academic studies raised awareness among individuals about why their data should be protected.

A person, who understands why his data should be protected, must then have the legal power to protect them. In this regard, the Law provides this legal power within the scope of right to personal data protection. Thanks to presence of a general and comprehensive Law, as well as a national authority to ensure such supervision and eventual proliferation of personal data protection, the individuals became aware of their rights and claimed for exercise of these rights. Prior to Law, individuals were impotent before data controllers and data processors; now, however, they are in a stronger position.

In practice, we observe individuals displaying a more interrogative attitude than before when they are asked to provide personal data. Today, we are asked to give our personal data by any party according to quality of our relation with such party. On some occasions, this is necessary for interest such as establishment and continuation of relationship or for realization of respective objectives of parties; sometimes, however, it can exceed this necessity. Upon such doubt, data subject inquiries why such information is asked from him and what will be done with the information. Accordingly, he refrains from providing his data if he cannot receive a satisfactory response. This is the level of awareness we need to establish.

### **What can a data subject do if his procedures will not be realized unless he provides data?**

Once data subject refrains from providing the demanded information, the data controller or data processor may indicate he cannot carry out the relevant procedure. In such case, the right of data subject to complain to Board will step in. Indeed, Board has made a declaration about high number of applications. These applications are settled in affirmative or negative manner, and the judgments are shared with public if deemed necessary.

An examination upon complaint of data subject may lead to two consequences: If, in the present case, data controller or data processor really needs such information in order to carry out the procedure in question and grounds on one of the conditions of processing foreseen in the Law, we cannot talk about a violation. Indeed, he demands the information for procedural requirements and not out of personal reasons. In such case, data subject should share such data if he wants to carry out the relevant procedure; if he does not want to share the data, then data subject should face and admit he cannot have his procedure accomplished. Nevertheless, in case data controller or data processor demands a data not necessary for the procedure in question, he can ground such demand only on explicit consent of data subject in line with the Law. Reluctance of data subject in providing information means he does not give explicit consent. At this point, his right to personal data protection is violated in case data controller or data processor does not carry out the procedure, for he was threatened with absence of the fulfillment if he does not give consent, whereupon the service is condition on statement of explicit consent. Such situation is a violation of right; it is not acceptable in the Law in any manner and it is considered unlawful by Board resolution.

## **Conclusion**

Right to personal data protection, which became a point of interest and attention in Turkey particularly after entry of relevant Law into force on 7 April 2016, is a field that concerns everyone by nature. As personal data is related with persons and information of persons, it is in touch with every field and sector. It covers all economic and commercial activities, as well as legal field, regardless of sector or section. Entry of the Law into force, the eventual legal regulations, activities by the Board and the law on personal data protection established upon Board resolution had an influence on every field and required update in consideration of this new approach on data protection law.

This is why we should try to grasp the meaning and importance of this new legal branch, rather than considering the consequences of personal data protection law as an additional burden. We should remember that law on personal data protection is a need in today's world and its consequences should be seen as an opportunity keep up with the times. In this context, we should try to comprehend the essence of law on personal data protection in every activity, particularly in process of Law compliance. This essence should be taken into account in any kind of activity in order to establish personal data protection as a culture.