http://dx.doi.org/10.12775/CLR.2025.008

Faik Tanrikulu*

COMPARATIVE EVALUATION OF SELECTED ELEMENTS OF DATA PROTECTION REGULATIONS: TÜRKIYE'S KVKK AND THE EU'S GDPR

Abstract

The rapid increase in digitalization and the widespread sharing of data has made the protection of personal data an important issue. This study aims to analyse the current practices regarding the protection of personal data in Türkiye in a comparative manner with the regulations adopted at international and European level. The study evaluates the effectiveness of the Law KVKK in Türkiye and offers suggestions on how this law can be aligned with international standards such as the EU's General Data Protection Regulation (GDPR). Based on important regulations such as the GDPR and the OECD's Data Protection Principles, the study aims to analyse the legal and policy instruments in Türkiye in depth. The similarities and differences between the GDPR and the LPPD are emphasized, especially on issues such as data transfer abroad, data processing processes and protection of sensitive data. The study analyses the process of aligning Türkiye's personal data protection regulations with EU standards and develops forward looking policy recommendations in terms of data security in the digital age.

Keywords

personal data protection – GDPR compliance – Turkish data protection law – data privacy – data security

* Assoc. Prof. Dr Faik Tanrikulu, Istanbul Medipol University Istanbul, Türkiye, ORCID: 0000-0002-0654-3140, e-mail: ftanrikulu@medipol.edu.tr.

Introduction

The protection of personal data is of much greater importance than in the past owing to the rapidly increasing data traffic in the digital world and the ever-increasing prominence of individuals' digital traces. Today, people share personal information through the traces they leave on social media, commerce, and other digital services. While this data is used for business decisions, political analyses and various strategic goals, it also comes with the risk of misuse. This raises awareness on the protection of personal data and forces governments and international organizations to act.

In the information age, personal data is referred to as the 'new oil' and has great economic value. However, as the misuse of data has the potential to damage the privacy of individuals, data security and privacy debates are becoming increasingly central. While the speed and ease of processing provided by technology has made it possible to collect and process personal data on a wider scale, it has also made it necessary to develop effective regulations for the protection of these data. The protection of personal data is considered as a means of protecting, not only the privacy of individuals, but also the security and stability of democratic societies. Protection of personal data is one of the most important issues today as it was in the past. On the one hand, with the developments in information and communication technologies today, practices for the collection, processing and storage of personal data are becoming more important. On the other hand, the ease and speed of processing brought about by advanced technology also brings up discussions on the protection of personal data. In this study, it is aimed to examine the basic legal regulations and practices regarding the protection of personal data and ensuring data privacy. In particular, the EU's General Data Protection Regulation (GDPR) and Türkiye's Personal Data Protection Law (KVKK) will be discussed as important examples in terms of data security and protection of individual rights. In Türkiye's aligning process with the EU, similarities and differences between GDPR and KVKK will be revealed, and light will be shed on national and international developments in the field of personal data protection.

By enacting the GDPR in 2018, the EU redefined data protection standards at the global level and established the most comprehensive legal framework regulating this field. The GDPR requires, not only the protection of data belonging to EU citizens, but also the compliance of all organizations processing such data worldwide. This makes it important for EU candidate countries such as Türkiye to align their data protection laws with European standards. In this context, the KVKK, which Türkiye enacted in 2016, follows similar principles with the GDPR and is considered as an important part of the aligning process with the EU.

This article will analyse the similarities and differences of these two regulations in terms of individual rights, data security, liability, and sanctions by comparing GDPR and KVKK. At the same time, the steps to be taken to ensure alignment between these two regulations and Türkiye's aligning process with EU data protection standards will be discussed. Personal data protection not only guarantees the privacy rights of individuals, but also has a great importance for the sustainability of the digital economy and democratic processes. Therefore, the regulations developed by states and international organizations in this field have become one of the basic building blocks of the digital age.

I. Law No. 6698 on the Protection of Personal Data Entered into Force

The drafting process for the Law on the Protection of Personal Data in Türkiye started in 2011, but the enactment process took quite some time. The enactment of this draft law was seen as an important step, especially within the framework of the European Union accession negotiations and for the comprehensive protection of personal data KVKK, 2016. The existence of a legal gap in the protection of personal data in the country has led to growing public outcry and citizens have become more vocal in their demands. This situation has made the necessity of a comprehensive personal data protection law even more evident.[1] Although the 2014 Law on the Regulation of Electronic Commerce is recognised

[1] Republic of Türkiye, *Law on the Protection of Personal Data*, Law No. 6698, 24 March 2016, Official Gazette No. 29677, 7 April 2016.

as an important step towards the protection of personal data in areas related to electronic commerce, this law provided protection for only a specific sector. Therefore, there was still a need for a general and inclusive personal data protection law.[2] In April 2016, the Law on the Protection of Personal Data was adopted and entered into force. This law, together with the Constitution and other legal regulations, created a legal framework that includes comprehensive measures for the protection of personal data. The law provided a strong legal framework to protect the privacy of individuals and prevent unlawful processing of personal data. This was a critical milestone for Türkiye to fulfil its international obligations and meet citizens' demands for the protection of their personal data. Enacted in 2016, KVKK is largely similar to the draft law prepared in 2011. Many articles of the Law were generally welcomed by the public and considered as an important step in the field of personal data protection. However, some parts of the law have also been criticized. In particular, it has been criticized that insufficient guidance is provided on issues such as data processing processes and the obligations of data controllers, and that some articles create uncertainty in practice.[3] The scope of application of the Law covers all data processing activities without any distinction between the public and private sectors. In this respect, the LPPD has determined the procedures and principles regarding the processing of personal data for both public institutions and private sector organizations, thus finding a wide application area. The Law aims to protect the privacy of individuals by stipulating strict controls and obligations in the processes of processing, storing, and sharing personal data with third parties. It also aims to ensure that personal data are processed in accordance with the law and data security is ensured through the obligations imposed on data controllers. The LPPD has been recognised as an important legal regulation on the protection of personal data in Türkiye. The Law's comprehensive and cross sectoral scope of application is an important step towards raising Türkiye's personal data protection standards to the international level. One of the most important provisions of the Law on the Protection of Per-

---

[2] Republic of Türkiye, *Law on the Regulation of Electronic Commerce*, Law No. 6563, 23 October 2014, Official Gazette No. 29166, 5 November 2014.

[3] Republic of Türkiye, *Law on the Protection of Personal Data*, Law No. 6698, 24 March 2016, Official Gazette No. 29677, 7 April 2016.

sonal Data is that it does not allow any personal data to be processed or shared with third parties without the explicit consent of the individual. This is one of the basic principles of the Law, which aims to protect the privacy and data security of individuals. Article 6 of the Law imposes serious restrictions on the processing of special categories of data. These special categories of data include race, ethnic origin, political opinion, philosophical belief, religion, sect, or other beliefs, clothing preferences, membership of associations, foundations or trade unions, health information, sexual life, criminal convictions and security measures, and biometric and genetic data. This article of the Law aims to secure the protection of such sensitive information by enabling the processing of special categories of personal data only under certain conditions. For example, the processing of such data may only be carried out in exceptional circumstances stipulated in the law or with the explicit consent of the individual. Thus, the law establishes a strong legal framework for the protection of individuals' privacy and prevents the use of such sensitive information by unauthorized persons. Furthermore, regarding the processing of special categories of data, the law emphasizes that such data require a higher level of protection and imposes additional obligations on data controllers. In this context, data controllers are obliged to take necessary technical and administrative measures during the processing of special categories of data. These provisions of the Law should be considered as part of the efforts to align Turkish legislation in the field of personal data protection with international standards. KVKK grants significant powers to the Personal Data Protection Board (Board) in cases of personal data breach or complaints. The Law authorizes the Board to examine and decide on complaints and to take necessary measures by evaluating alleged violations. In this context, the Board supervises whether personal data are processed in accordance with the law and is authorized to take necessary measures in case of a violation. When the Board detects a violation of rights, it is authorized to take provisional measures by requesting the remedy of the violation within thirty days. These powers are of great importance in terms of ensuring the applicability and effectiveness of the law. These sanction mechanisms of the law aim to ensure that the protection of personal data does not remain only at the theoretical level, but also effectively in actual practice. In this respect, the Law obliges data controllers to pro-

cess personal data in accordance with the law and provides for serious sanctions when necessary.

1. Amendments to Law No. 6698 and Future Directions

Recent amendments to the Law No. 6698 on the Protection of Personal Data have revealed the necessity to make more comprehensive and up to date regulations on the protection of personal data with the rapidly increasing impact of digitalization. These amendments made in 2024 were made to ensure data security at both national and international level, as data breaches and personal data processing activities have become more complex with the development of technology. First, the Law on the Amendment of the Code of Criminal Procedure and Certain Laws, published in the Official Gazette on 12 March 2024, contains new provisions regarding Law No. 6698 on the Protection of Personal Data. These amendments aim to protect the privacy of individuals more effectively in the age of digitalization and to create a more transparent and accountable structure in data processing processes. The amendments introduce radical changes to Articles 6, 9 and 18 of the Law, and reregulate the procedures and principles regarding the transfer of personal data abroad. Article 9 introduces new criteria for more secure processing of personal data in international data transfers. It is stated that data transfers abroad can be made only with countries that provide adequate protection, otherwise the approval of the Board must be obtained. However, the entry into force of this regulation has been postponed until 1 September 2024, which allows companies to carry out the necessary compliance studies in this process. [4] With these amendments, KVKK has been given broader powers and stricter sanctions are envisaged in case of violations. In the new version of the law, companies are required to implement corrective measures within thirty days in the case of detection of data breaches, otherwise they are likely to face heavier administrative fines. These sanctions aim to ensure greater security and transparency in the processing of individuals' data. The newly

[4] Republic of Türkiye, *Law on the Amendment of the Code of Criminal Procedure and Certain Laws*, Law No. 7499, 12 March 2024, Official Gazette No. 32487, 12 March 2024.

added temporary article allows personal data processing activities to be managed under more flexible rules for a certain period. This temporary regulation aims to provide an adaptation process for data processing institutions, especially in the face of new challenges brought by digitalization.

In conclusion, these amendments constitute one of the important steps taken by Türkiye for the protection of personal data in the era of digital transformation. The adoption of a more comprehensive and effective regulation against data security threats with developing technologies is an important milestone in the process of both protecting the rights of individuals and aligning Türkiye with international data protection standards.

2. Comparison of Data Protection Supervisory Authorities in the EU and Türkiy

The effectiveness of data protection systems depends, not only on the existence of legal regulations, but also on the presence of independent and strong supervisory authorities that ensure their implementation. In the European Union, this function is carried out under the GDPR by national data protection authorities and coordinated by the European Data Protection Board (EDPB). In Türkiye, this role is undertaken by the Personal Data Protection Authority and its Board. Articles 51–59 of the GDPR require supervisory authorities in member states to operate in accordance with the principle of full independence.[5] These authorities have the power to investigate violations, audit data controllers, issue binding decisions, impose administrative fines, and publish guidelines at both the national and EU levels.[6]

In the European Union, the supervisory and regulatory authority in the field of data protection and digital services is exercised by the European Data Protection Board (EDPB) and the national data protection

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*), OJ L 119, 4.5.2016, supra note 1, art. 51–52.

[6] *Ibid*., art. 57–58.

authorities of the member states. The EDPB monitors the implementation of the GDPR and ensures the consistent application of data protection policies across the EU. In addition, under the Digital Services Act (DSA), Digital Services Coordinators (DSC) are responsible for overseeing the compliance of digital service providers and reporting potential breaches. In Türkiye, the Personal Data Protection Authority assumes a similar role to the GDPR in Europe, ensuring the protection of personal data and enacting regulations on this issue. KVKK supervises data breaches and imposes sanctions when necessary. Türkiye is also updating its regulations on digital services to align with EU standards. Although the supervisory authorities in Türkiye and the EU have certain similarities in terms of functioning and duties, it is observed that both structures operate with different legal frameworks and implementation approaches.

Table 1. Comparison of Supervisory Authorities in the EU and Türkiye

Criteria	EU	Türkiye
Main Regulatory Framework General Data	Protection Regulation (GDPR), Digital Services Act (DSA	Personal Data Protection Act (KVKK)
Supervisory Authorities European Data	Protection Board (EDPB), Digital Services Coordinators (DSC)	Personal Data Protection Authority (KVKK)
Duties and Authorities Supervising	The implementation of GDPR and DSA, reporting data breaches, applying criminal sanctions	Supervising the implementation of KVKK, reporting data breaches, applying criminal sanctions
International Cooperation	The EU Commission encourages the aligning of the Digital Services Act (DSA) in candidate and potential candidate countries.	Türkiye continues its cooperation with the EU in the field of data protection and digital services and updates its regulations to comply with international standards. KVKK regulates international data transfers.

Table 1. Comparison of Supervisory Authorities in the EU and Türkiye

Criteria	EU	Türkiye
Education and Awareness Raising	In the EU, Digital Services Coordinators (DSC) and other relevant authorities organize various campaigns and offer training programmes to inform citizens and businesses about digital services law and data protection.	In Türkiye, the PDPL organizes training programmes, seminars, and public information campaigns to raise awareness on data protection. KVKK aims to raise awareness of citizens and organizations on data protection.

In addition, the GDPR adopts the one stop shop principle in cases involving cross border data processing activities, designating the supervisory authority of the country where the data controller's main establishment is located as the lead authority. This system ensures both consistency and swift decision making. Similarly, in Türkiye, the Personal Data Protection Authority oversees the implementation of data protection legislation, evaluates breach notifications, imposes administrative fines, may decide to suspend data processing activities, and publishes guidance documents.[7] However, unlike the multifactor and coordination based structure at the EU level, the KVKK Authority has been only partially integrated into international cooperation mechanisms. For example, its absence from a permanent international coordination platform like the EDPB limits Türkiye's role, particularly in cross border data transfers and joint supervisory projects. Moreover, GDPR supervisory authorities place significant emphasis, not only on their investigative and enforcement powers, but also on guidance and awareness raising activities. The EDPB and national authorities regularly issue sector specific guidelines, best practice documents, and risk assessment methodologies. While the KVKK Authority has increased the number of its guidance documents in recent years, the scope of sector specific and

[7] 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7.4.2016, No. 29677, art. 21–22.

technically focused guidance initiatives still holds considerable potential for expansion.

To align with EU standards and enhance the effectiveness of the supervisory authority, the following steps could be prioritized:

- international coordination: enabling the KVKK Authority to participate as an observer or associate member in platforms similar to the EDPB would strengthen cross border cooperation;
- topshop–like mechanism: a centralized lead authority model could be developed to facilitate application and inspection processes for multinational data controllers.
- sectoral expertise units: specialized units could be established for auditing and providing guidance in high-risk sectors such as finance, healthcare, ecommerce, and artificial intelligence;
- proactive supervision: proactive inspections based on risk analysis should be expanded, focusing, not only on post breach interventions, but also on preventing breaches.

In the context of EU data protection enforcement, a number of landmark administrative and judicial decisions have significantly influenced the interpretation and practical application of the GDPR, particularly in relation to international data transfers, transparency obligations, and the lawful basis for processing personal data. One of the most prominent cases is the Court of Justice of the European Union (CJEU) ruling in *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, which invalidated the EU–US Privacy Shield framework on the grounds that U.S. surveillance laws did not provide an adequate level of protection equivalent to that guaranteed within the EU.[8] At the national level, supervisory authorities have issued several high-profile decisions. For instance, the Commission Nationale de l'Informatique et des Libertés (CNIL) imposed a €50 million fine on Google LLC in 2019 for failing to provide users with sufficiently clear and comprehensive information about data processing for advertising personalization, and for not obtaining valid consent in accordance with

[8] *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18, Judgment of 16.7.2020, ECLI:EU:C:2020:559, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 [last accessed 10.8.2025].

Articles 6 and 7 GDPR.[9] Similarly, the UK Information Commissioner's Office (ICO) fined British Airways £20 million in 2020 after a cyberattack exposed the personal data of more than 400,000 customers, citing the airline's failure to implement appropriate technical and organizational measures as required under Article 32 GDPR.[10]

These examples illustrate how both the CJEU and national supervisory authorities actively interpret and enforce the GDPR, setting precedents that guide data controllers and processors across the EU. For countries such as Türkiye, which aim to align the Law on the Protection of Personal Data (KVKK) with the GDPR, these rulings provide valuable insights into the standards and expectations that may shape future domestic enforcement practices.

In conclusion, having supervisory authorities that are independent, strong, and open to international engagement is a critical factor directly affecting the credibility of a data protection system. Enhancing the institutional capacity of the KVKK Authority would serve as a positive indicator in Türkiye's process of obtaining an EU adequacy decision and would also strengthen the country's reputation in the digital economy.

II. Definition of Cybersecurity Regulations

Cybersecurity is not merely a technical requirement in personal data protection law, but also a fundamental element that ensures the enforceability and credibility of the legislation. A personal data breach not only undermines individuals' privacy, but also directly threatens national security and economic stability in critical sectors such as finance, healthcare, energy, and public administration. Therefore, both the European

---

[9] Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération de la formation restreinte n° SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC*, Légifrance, published 22 January 2019, available at: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552 [last accessed 10 August 2025].

[10] Information Commissioner's Office (ICO), penalty for British Airways (BA) data breach – fine of £20 million for insufficient data protection measures after 2018 cyber-attack affecting ~400,000 customers, confirmed by GDPR Hub summary, available at: https://www.gdprregister.eu/news/british-airways-fine/ [last accessed 10.8.2025].

Union's GDPR and Türkiye's KVKK impose explicit obligations on data controllers and processors to ensure cybersecurity.

Article 32 of the GDPR requires data controllers and processors to implement "appropriate technical and organizational measures" taking into account the nature, scope, context, and risk level of the processing activity. These measures include pseudonymization, anonymization, strong encryption techniques, system access controls, physical security safeguards, regular security testing, and audit mechanisms. The GDPR also mandates that, in the event of a data breach, it must be reported to the supervisory authority within no more than 72 hours. This timeframe ensures both transparency and the ability to respond promptly.[11]

Article 12 of the KVKK likewise imposes an obligation on data controllers to "take all necessary technical and administrative measures" to ensure the security of personal data.[12] However, unlike the GDPR, the KVKK does not detail technical measures in the text of the law itself, instead leaving their definition and scope to the guidelines and decisions of the Personal Data Protection Board. In its published "Guide on Technical and Administrative Measures Regarding Data Security," the Board recommends practices such as encryption, keeping log records, conducting penetration tests, and providing staff training; however, these measures are not legally binding at the statutory level. EU legislation, moreover, addresses cybersecurity, not only within the GDPR framework, but also through the NIS Directive (Directive on Security of Network and Information Systems) and, more recently, the NIS2 Directive. NIS2 imposes mandatory cybersecurity standards and incident reporting deadlines on organizations operating in critical sectors such as energy, transport, health, digital infrastructure, public administration, and finance. This integration ensures that data protection law functions in harmony with national and EU level cybersecurity policies. In Türkiye, cybersecurity regulations are supported outside the KVKK by the *National Cybersecurity Strategy and Action Plan (2020–2023)*, coordinated by the Ministry of Transport and Infrastructure, and by the activities of the *National Cyber Incident Response Centre* (USOM). However, the institutional connection between this national strategy and the KVKK re-

---

[11] General Data Protection Regulation, art. 33.

[12] 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7.4.2016, No. 29677, art. 12.

mains underdeveloped. For example, regarding data breach notifications, the KVKK uses the more flexible phrase "as soon as possible," whereas national cybersecurity protocols in certain sectors require reporting within 24 or 48 hours. This lack of alignment can create confusion in practice.[13]

For Türkiye to establish a robust cybersecurity regime aligned with EU standards, the KVKK should explicitly define a clear data breach notification deadline adopting, as in the GDPR, a maximum limit of 72 hours. Technical measures such as encryption, access management, logging, penetration testing, and data minimization should be explicitly listed in the text of the law and made legally binding. Mandatory cybersecurity protocols, similar to the NIS2 model, should be introduced for critical sectors such as energy, health, finance, and telecommunications. An institutional cooperation mechanism should be established between the KVKK Authority and USOM for data breach notifications and risk assessments, and cybersecurity certification systems should be expanded, making independent audit processes compulsory. Clearly, comprehensively, and bindingly defining cybersecurity regulations is indispensable, not only for the protection of personal data, but also for the security of critical national infrastructure. Türkiye's integration with the EU in the field of data protection and the attainment of an adequacy decision are directly linked to harmonizing its cybersecurity regulations with GDPR and NIS2 standards.

1. Transfer of Personal Data to Third Countries

The transfer of personal data to third countries is one of the most sensitive areas of data protection law. While the operation of the digital economy on a global scale makes cross border data flows inevitable, ensuring that these flows are carried out securely has become a fundamental requirement both for the protection of individual rights and for the sustainability of international trade. In this context, both the Euro-

---

[13] H. Çakır, S.A. Uzun, "Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi (2013-2014, 2016-2019 ve 2020-2023)", *Ekonomi, İşletme, Siyaset ve Uluslararası İlişkiler Dergisi (JEBPIR)*, vol. 7, no. 2, 2021, p. 353, available at: https://dergipark.org.tr/tr/download/article-file/2018494 [last accessed 9.8.2025].

pean Union's GDPR and Türkiye's Law KVKK adopt the principle of an "adequate level of protection" for transfers to third countries; however, they differ significantly in the methods of implementing this principle.

Articles 44–50 of the GDPR regulate the transfer of personal data outside the European Union within the framework of three main legal bases:

- an adequacy decision by the European Commission,
- appropriate safeguards (such as Binding Corporate Rules, Standard Contractual Clauses, and accreditation mechanisms),
- the explicit consent of the data subject under certain exceptions.[14] Under the GDPR, explicit consent may serve as a legal basis for the transfer of personal data even to countries that do not ensure an adequate level of protection; however, such consent must be informed, freely given, and explicit.[15] In addition, the GDPR requires that, for transfers based on such consent, the data subject must be provided with clear and comprehensible information about the potential risks of the transfer.

Article 9 of the KVKK, on the other hand, adopts a more restrictive approach to the transfer of personal data to third countries. Under this provision, cross border data transfers may be carried out only with the explicit consent of the data subject or to countries declared by the Personal Data Protection Board to have an adequate level of protection. Transfers to countries lacking adequate protection are permitted only if the data controllers in Türkiye and in the relevant foreign country provide a written undertaking of adequate safeguards, and this undertaking is approved by the Board .[16] This system, by requiring Board approval for each transfer scenario, makes the administrative process more burdensome compared to the GDPR. The practical implications of these differences are significant. While the GDPR offers flexible mechanisms such as the use of standard contractual clauses without prior approval to facilitate transfers outside the European Economic Area, the procedure under the KVKK can create additional administrative burdens and delays, particularly in intragroup

---

[14] General Data Protection Regulation, art. 44–46.

[15] *Ibid*., art. 49(1)(a).

[16] 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7.4.2016, No. 29677, art. 9(2).

data transfers by multinational companies. This situation emerges as an obstacle that should be taken into account in Türkiye's process of obtaining an EU adequacy decision, since the European Commission evaluates, not only legislative alignment, but also practical effectiveness and procedural ease in its adequacy assessments. Another critical difference in international data transfers lies in the scope of exceptions. The GDPR permits transfers on grounds such as public interest, the establishment, exercise or defence of legal claims, the protection of vital interests, or where necessary for the requirements of international agreements. [17] In the KVKK, these exceptions are defined within a much narrower scope, which can limit Türkiye's capacity for international cooperation and data sharing.

While the KVKK's third country transfer provisions offer strong safeguards for data security, they do not reach the level of flexibility envisioned by the GDPR. For Türkiye to achieve deeper integration with the EU in the field of data protection and to obtain an adequacy decision, the balance between explicit consent, appropriate safeguards, and administrative approval mechanisms needs to be restructured. In this context, adapting tools such as Binding Corporate Rules and Standard Contractual Clauses as provided for in the GDPR, in a way that ensures wider use and accelerates approval processes, would enhance both legal alignment and international competitiveness.

2. Expansion of Special Category Personal Data Protection Standards and EU Harmonization Process

Special categories of personal data are those that can directly affect individuals' fundamental rights and freedoms, and whose processing may pose serious risks such as discrimination, stigmatization, or loss of rights. For this reason, both the European Union's GDPR and Türkiye's Law KVKK impose stricter conditions on the processing of such data compared to general categories of personal data. Article 9 of the GDPR defines special categories of data as including: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union mem-

[17] General Data Protection Regulation, art. 49(1)(c)-(g).

bership, genetic data, biometric data, health data, and data concerning a person's sex life or sexual orientation.[18] The processing of such data is, as a rule, prohibited. By way of exception, processing is permitted on legal grounds such as the explicit consent of the data subject, the fulfilment of employment and social security obligations, the protection of the vital interests of the data subject, obligations based on public interest, the provision of healthcare services, and medical research activities.[19] The GDPR also requires that a Data Protection Impact Assessment (DPIA) be carried out when processing such data, and that preventive measures be implemented to mitigate the identified risks.[20]

Article 6 of the KVKK defines a broader list of special categories of personal data compared to the GDPR: race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and attire, membership of associations/foundations/trade unions, health information, sexual life, criminal convictions and security measures, as well as biometric and genetic data.[21] In the KVKK, such data may be processed only with the explicit consent of the data subject or under limited exceptions provided by law. The processing of health and sexual life data is permitted solely for purposes such as protecting public health, preventive medicine, medical diagnosis and treatment, and the planning and financing of healthcare services.

Two key differences emerge here:

- scope of exceptions: the GDPR allows broader exceptions such as public interest and scientific research, whereas the KVKK keeps these areas highly restricted. This significantly hinders, for example, the sharing of health data from Türkiye in international academic research projects;
- normative level of technical measures: the GDPR explicitly specifies in its legislative text technical measures such as pseudonymization, anonymization, and data minimization when processing special categories of data.[22] In contrast, the KVKK does not im-

---

[18] *Ibid*., art. 9(1).

[19] *Ibid*., art. 9(2)(a)-(j).

[20] *Ibid*., art. 35.

[21] 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7.4.2016, No. 29677, art. 6(1).

[22] General Data Protection Regulation, art. 4(5), 25.

pose a clearly defined maximum period for breach notification, instead requiring that it be done "as soon as possible."

This vagueness can lead to delays in reporting and hinder timely mitigation measures, particularly in cases involving high risk categories of personal data. Aligning the KVKK with the GDPR by introducing explicit obligations such as mandatory DPIAs for high risk processing, a fixed breach notification window, and the codification of specific technical safeguards would significantly strengthen Türkiye's compliance framework and facilitate progress toward obtaining an EU adequacy decision.[23] In the KVKK, however, this period is vaguely defined as "as soon as possible," which weakens legal predictability for data controllers and constitutes a negative indicator in the EU harmonization process. In the light of all these differences, it is critically important for Türkiye to strengthen the KVKK's provisions on the protection of special categories of personal data in the context of alignment with the EU's data protection framework. In particular:

- the scope of exceptions should be broadened in line with the GDPR, and the transfer of data for scientific research, public interest, and international cooperation projects should be legally safeguarded;
- technical protection measures should be defined at the legislative level and made binding;
- breach notification periods should be set as fixed and measurable timeframes, as in the GDPR;
- the obligation to conduct impact assessments should apply to all types of processing involving special categories of personal data and be subject to administrative oversight;
- the protection of special categories of personal data is not merely a subfield of data protection law, but also a critical instrument in realizing the principles of privacy and the prohibition of discrimination, which form the foundation of a democratic social order. The framework introduced by the GDPR, not only secures individuals' rights but also imposes high levels of transparency, accountability, and preventive security measures on data controllers. While the KVKK's current provisions appear close to the

[23] *Ibid.*, art. 33.

GDPR in terms of general protection principles, the narrowness of the exceptions, the lack of codified technical measures at the legislative level, and the ambiguity of breach notification processes place Türkiye behind in both enforcement effectiveness and legislative alignment with the EU. Strengthening these provisions would be strategically important, not only for obtaining an "adequacy decision" from the EU, but also for facilitating participation in international academic collaborations, ensuring the secure sharing of health data in medical tourism, enhancing data security in the finance and biotechnology sectors, and easing the operations of multinational companies in Türkiye.

3. Similarities and Differences between Turkish Personal Data Protection Law and EU GDPR

The LPPD, which entered into force in 2016 and was revised in 2024, is seen as a historical and important milestone for Türkiye. It is in parallel with the GDPR, which entered into force in Europe in a similar manner and contains similar provisions. It is of great importance for both the EU and Türkiye in terms of protecting the privacy rights of individuals with processes such as the collection, processing, and storage of personal data. This law creates an umbrella that secures many individual rights in order to protect the personal data of individuals. In both regions, the right to access, rectify, and even delete data is recognised. The PDPL also introduces important innovations in terms of requiring data processing organizations to take the necessary security measures and providing sanctions through supervisory bodies such as the Personal Data Protection Authority in the case of data breach. The 2024 amendments to the KVKK stand out as one of the important steps Türkiye has taken towards aligning its data protection regulations with global standards, especially the GDPR. In today's world where digitalization is accelerating, the protection of personal data has necessitated regulations to protect the rights of individuals and to increase data security. One of the most important updates made in this context is the conditions for processing special categories of personal data. In general, sensitive personal data such as race, ethnic origin, political opinion, reli-

gion, health information, and biometric data cannot be processed without the explicit consent of the data subject. However, in an emergency, such as an individual's health condition, it may become necessary to access health information, for example, to protect the life of a person who is unable to give consent. This regulation, in line with the GDPR, introduces exceptions that allow the processing of sensitive data in mandatory cases. Similar regulations in the GDPR prevent data processing without the consent of individuals, while allowing data processing in critical situations such as public health and security. The issue of data transfer abroad is another important update. With the amendments made to Article 9 of the LPPD, an 'adequacy decision' is sought for data transfers abroad and it is assessed whether the country of data transfer has adequate data protection standards. As in the GDPR, data transfer to countries that do not have adequate protection can be possible only if security measures such as binding corporate rules (BCR) or standard contractual clauses (SCC) are provided. This regulation is of great importance for Turkish companies to operate internationally and especially to share data with the European Union. Administrative sanctions have also been increased in line with the GDPR. In the event of a data breach during the processing of personal data, the penalties to be applied in cases such as failure to notify the relevant institutions or failure to ensure personal data security have been significantly increased. As in the GDPR, fines for data breaches can be up to 4% of annual revenue. In Türkiye, on the other hand, more reasonable penalties are stipulated in the KVKK, but it is seen that these penalties have also been increased with the new regulations. Data breaches may have significant financial consequences, especially for companies that transfer data internationally. In addition to these regulations, the responsibilities of data processors who transfer data abroad have also been increased. While only data controllers were subject to these obligations in the previous regulations, the new regulation requires data processors to bear the same responsibilities when transferring data abroad. This obliges companies to carry out their data processing processes with third parties more carefully. The new regulation also makes it possible to impose criminal sanctions in cases where data processors do not take adequate security measures during data transfer abroad. Within the scope of the amendments, training and awareness activities are also of great importance.

Raising the awareness of all employees involved in the data processing process about these regulations stands out as a critical step to prevent possible violations. In addition, reviewing existing data processing processes and aligning these processes with the new regulations is important for companies to minimize the risks they may face. These amendments will increase the competitiveness of Türkiye's data protection regime at the global level and provide a more secure and align data protection infrastructure for Turkish companies operating internationally. These GDPR-aligned regulations will strengthen both Türkiye's relations with the EU and the country's global position in the field of data protection. These innovations introduced to the Turkish Personal Data Protection Law, not only strengthen the data security of individuals, but also facilitate international data transfers and integration into global business processes. Therefore, both large scale enterprises and small and medium sized enterprises (SMEs) should quickly adapt to these new regulations and act by considering the security standards set in their data processing activities.[24]

Faruk Bilir, President of the Personal Data Protection Authority, stated the following in an interview about the KVKK, which entered into force in April 2016 and amended the relevant law in 2024: 'The law is based on the European Union Data Protection Directive, which ensures unity of practice among European countries in the protection of personal data. In 2018, two years after our Law entered into force, the Directive was repealed and the European Union GDPR, which contains more comprehensive regulations in terms of the protection of personal data, was put into effect. In addition, Bilir said, 'As a result of aligning with the European Union acquis, adaptation to the innovations brought by the developing technology and new approaches adopted on international platforms, as well as the needs arising in practice, important amendments have been made to the relevant articles regulating the conditions for processing special categories of personal data, data transfer abroad, and misdemeanours regarding the protection of personal data. These amendments were published in the Official Gazette dated 12 March 2024 and entered into force on 1 June

[24] Republic of Türkiye, *Law on the Amendment of the Code of Criminal Procedure and Certain Laws*, Law No. 7499, 12 March 2024, Official Gazette No. 32487, 12 March 2024.

2024,' and pointed out important changes, especially in terms of EU GDPR compliance.[25]

However, Article 9 of the Law is seen as the most fundamental aligning legislation in terms of EU aligning. According to President Faruk Bilir, 'Article 9 of the Law has been amended based on the relevant provisions of the GDPR. A new system has been introduced for data transfer abroad. As a first step, it should be checked whether there is an adequacy decision. An adequacy decision is issued by the Board and may be issued about a country, international organization, or sectors. If there is no adequacy decision, data can be transferred by providing appropriate safeguards. Appropriate safeguards include options such as a standard contract, binding corporate rules, or a letter of undertaking,' he added. Another important change concerns the long duration of judicial processes. Years of administrative and judicial processes cause delays in terms of justice. In this respect, the amendments to the Law authorise data processors to transfer data abroad. In addition, the application to the Criminal Judgeships of Peace against administrative fines has been abolished, and the possibility to apply to administrative courts has been introduced. Standard contracts regarding data transfer abroad must be notified to the Authority within five business days, otherwise administrative sanctions may be imposed.[26]

4. Sanctions to Be Applied in Case of Violation of Data Protection Provisions

The effectiveness of data protection legislation depends, not only on the normative determination of protection principles, but also on the deterrent effect of the sanctions to be applied in cases of noncompliance with these principles. For this reason, both the European Union's GDPR and Türkiye's KVKK provide for various administrative fines and other

---

[25] A. Ajansı, *"KVKK Başkanı Bilir: Kişisel Verilerin Korunması Kanunu'ndaki Değişiklikleri AA'ya Değerlendirdi"*, 15 June 2024, available at: https://www.aa.com.tr/tr/gundem/kvkk-baskani-bilir-kisisel-verilerin-korunmasi-kanunundaki-degisiklikleri-aaya-degerlendirdi/3250588 [last accessed 6 August 2025].

[26] Personal Data Protection Authority (KVKK), *Press Release on Amendments to the Law on the Protection of Personal Data*, 2024.

sanctions in the event of a violation of data protection provisions. However, there are significant differences between the two regulations in terms of the scope, amount, and procedures for implementing sanction mechanisms.

Article 83 of the GDPR stipulates two main categories of fines, depending on the nature of the violation:

- for less serious infringements, administrative fines of up to EUR 10 million, or up to 2% of the total worldwide annual turnover;
- for more serious infringements, administrative fines of up to EUR 20 million, or up to 4% of the total worldwide annual turnover.[27]

In addition, the GDPR stipulates that, when determining the amount of fines, factors such as the nature, duration, and scope of the infringement, the degree of intent or negligence, the extent of the damage caused to the data subject, the level of cooperation by the data controller, and any previous records of violations must be taken into account. This system aims to ensure that fines are both proportionate and dissuasive. Article 18 of the KVKK, on the other hand, provides for fixed amount administrative fines for violations. As of 2024, the maximum administrative fine that can be imposed for a breach of data security obligations is approximately 3 million Turkish Lira.[28]

This amount is particularly low in terms of deterrence when compared to the rates stipulated under the GDPR, especially for large companies operating on an international scale. Moreover, the KVKK does not contain a mechanism to proportionately adjust fine amounts according to the economic size of the data controller. Furthermore, under the GDPR, infringements are not limited to monetary fines; supervisory authorities may also issue binding administrative orders such as the suspension of data processing activities, the deletion of specific data sets, or the implementation of corrective measures. While the KVKK grants the Board similar powers to suspend or delete data processing activities, in practice, these powers are exercised less frequently and typically only in cases of severe violations.

In practice, these differences affect both the risk perception of data controllers and their motivation to prevent violations. The GDPR's high

---

[27] General Data Protection Regulation, art. 83(4)-(5).

[28] 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7.4.2016, No. 29677, art. 18.

value and proportionate penalty system encourages companies to continuously update their data protection compliance programs, whereas the KVKK's fixed amount penalty system can be perceived particularly by high revenue companies as a "payable cost." In the long term, this perception may negatively impact the establishment of a strong compliance culture.

For Türkiye to align with EU standards and enhance its international credibility in the field of data protection, it is necessary to adopt a proportional penalty mechanism based on a specific percentage of the annual turnover, as in the GDPR; to explicitly set out in the law criteria such as the severity of the infringement, recurrence, and elements of negligence or intent; to increase the frequency of applying corrective measures, suspension of activities, and data deletion orders in addition to monetary fines; and to support sanctions, not only with post violation measures, but also with preventive oversight mechanisms and sector specific guidance. In conclusion, ensuring that sanctions for breaches of data protection provisions are proportionate, dissuasive, and effective can safeguard not only individuals' rights, but also foster trust in the data economy. Strengthening the KVKK's sanction regime will also serve as an important indicator in Türkiye's process of obtaining an EU adequacy decision.

5. Material and Personal Scope of the KVKK and GDPR

5.1. Material Scope:

Article 2 of the Law on the Protection of Personal Data No. 6698 stipulates that the Law shall apply to "the processing of personal data wholly or partly by automated means or, provided that it is part of a data recording system, by nonautomated means.[29] This provision is binding for both public institutions and organizations as well as the private sector. The KVKK requires the protection of personal data regardless of the method of processing, as long as it is part of a specific recording system. However, Article 28 of the Law excludes certain situations from its

[29] Türkiye, *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, Resmî Gazete, 7.4.2016, m. 2.

scope. [30] These exceptions include processing activities carried out within the scope of national defence, national security, public security, public order, economic security, the privacy of private life, or the confidentiality of communications, as well as activities that are entirely personal or related to family matters.

Article 2 of the European Union's GDPR states that the Regulation applies to "the processing of personal data wholly or partly by automated means" and to "the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." However, the GDPR explicitly excludes certain areas of activity from its scope. Chief among these are personal data processing activities carried out for the purposes of the prevention, investigation, detection, and prosecution of criminal offences, and the execution of criminal penalties. Such activities do not fall under the GDPR, but are regulated under Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 ("Law Enforcement Directive").[31] The Directive contains specific provisions regarding data processing activities carried out by law enforcement authorities and establishes the data protection standards for such activities. The GDPR also excludes from its scope data processing activities carried out solely for personal or household purposes. In this way, activities that fall entirely within an individual's private life are exempt from the intervention of data protection legislation.

In the KVKK, data processing activities related to crime prevention, judicial investigations, and the enforcement of criminal sentences are not explicitly distinguished; however, activities falling within the scope of public security and national security are regulated as exceptions. In contrast, under EU law, this area is governed entirely by a separate legal instrument, the Law Enforcement Directive (Directive (EU) 2016/680), and should not be conflated with the GDPR. Therefore, in KVKK–GDPR comparisons, it should be emphasized that data processing for law enforcement purposes falls under the scope of the special Law Enforcement Data Protection Directive, not the GDPR.

---

[30] *Ibid*., m. 28.

[31] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, OJ L 119, 4.05.2016, pp. 89–131.

Table 2. Comparative Legal Scope of GDPR and KVKK

Scope Type	GDPR	KVKK
Material Scope	**Art. 2(1) –** Applies to the processing of personal data wholly or partly by automated means and to non-automated processing if the data forms part of a filing system or is intended to form part of one. **Art. 2(2) –** Excludes processing outside the scope of Union law, purely personal/household activities, and processing for law enforcement purposes under Directive (EU) 2016/680[32].	**Art. 2 –** Applies to natural persons whose personal data are processed, and to natural/legal persons who process such data wholly or partly by automated means or by non-automated means, provided that the process is part of a data recording system[33].
Personal Scope	**Art. 3(1) –**This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not , **Art. 3(2) –** Applies to controllers/processors not established in the Union if they offer goods/services to data subjects in the Union or monitor their behaviour within the Union[34].	**Art. 3 –**Applies to all natural persons whose personal data are processed, regardless of nationality or residence, and to all natural/legal persons who process such data, provided that processing occurs within the framework of a data recording system[35]

[32] General Data Protection Regulation, art. 2(1)-(2).

[33] Law No. 6698 on the Protection of Personal Data (KVKK), art. 2.

[34] General Data Protection Regulation, art. 3(1)-(2).

[35] Law No. 6698 on the Protection of Personal Data (KVKK), art. 3.

5.2. Personal scope

The KVKK applies to all natural and legal persons located in Türkiye or conducting data processing activities within Türkiye. However, the definition of the "data subject" protected under the Law refers solely to identified or identifiable natural persons.[36] Legal persons are not protected as data subjects under the KVKK. This means that information belonging to commercial companies or public legal entities falls outside the scope of KVKK protection. The GDPR applies to data controllers and processors located within the European Union, as well as to organizations established outside the EU that offer goods or services to data subjects in the EU or monitor their online behaviour (Art. 3).[37] The GDPR likewise provides protection only for natural persons, and data relating to legal persons falls outside the scope of this protection.[38] One of the most significant aspects of the GDPR's personal scope is its "extraterritorial" application to data controllers located outside the EU.[39] This means that any organization processing the personal data of EU data subjects, regardless of its geographical location, may be subject to the GDPR. The comparison of the material and personal scope of the KVKK and the GDPR reveals that, although both regulations are built on similar principles, they differ significantly in terms of their scope of application and exceptions. The KVKK provides broad exemptions in areas such as public security and national security, whereas the GDPR completely excludes personal data processing activities related to crime prevention and criminal justice from its scope and regulates these matters under Directive (EU) 2016/680. Both regulations provide protection only to natural persons, and data relating to legal entities remains outside their scope. The GDPR's extraterritorial applicability establishes a global standard in the field of data protection, while alignment steps to be taken by the KVKK in this regard would contribute to positioning Türkiye as a reliable regime for international data transfers.

---

[36] KVKK, m. 2.

[37] General Data Protection Regulation, art. 3.

[38] *Ibid*., Recital 14.

[39] *Ibid*.

6. Processing of Personal Data for the Purpose of Combating Crime and EU Directive 2016/680

In the European Union data protection regime, the processing of personal data for the purposes of combating crime and criminal justice is excluded from the scope of the GDPR. Article 2(2)(d) of the GDPR explicitly provides that the Regulation shall not apply where such activities are carried out "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."[40]

This area is specifically regulated by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (the Law Enforcement Directive – LED).[41] The purpose of the LED is to ensure the protection of personal data processed by competent authorities in the context of criminal justice and law enforcement activities, while also establishing common standards for the cross border sharing of such data.

The Directive:

- sets out data processing principles (lawfulness, data minimization, purpose limitation, etc.);
- defines the rights of data subjects (access, rectification, erasure);
- establishes data security measures and oversight mechanisms in detail.[42]

The key distinction between the LED and the GDPR lies in their scope, which is based on the purpose of processing: the GDPR essentially covers personal data processed in the private sector and in the administrative activities of the public sector, whereas the LED regulates only data processing in the fields of criminal justice and law enforcement. Therefore, within the EU, data protection legislation operates along two separate axes, and the processing of personal data for law enforcement purposes cannot legally be considered under the GDPR.

In Türkiye, by contrast, the KVKK provides exemptions in areas such as national security, public security, and public order (Art. 28), but

---

[40] General Data Protection Regulation, art. 2(2)(d).

[41] European Union, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, OJ L 119, 4 May 2016, pp. 89–131.

[42] *Ibid*., art. 4–8.

there is no separate law on law enforcement data protection as in the EU. This points to a legislative gap that Türkiye should take into account in its future alignment process with EU standards.

7. Legal Grounds for Data Processing and Consent Requirement in Crossborder Data Transfers

In both Turkish and European Union law, personal data processing activities are considered lawful only if specific legal grounds exist. Pursuant to Article 5 of the Law on the Protection of Personal Data No. 6698, personal data may be processed either with the explicit consent of the data subject or in the presence of one of the exceptional circumstances enumerated in the law.

These exceptions are as follows:

- where it is expressly stipulated by law;
- where it is necessary to protect the life or physical integrity of the person who is unable to give consent owing to actual impossibility, or whose consent is not legally valid, or of another person;
- where it is directly related to the establishment or performance of a contract;
- where it is necessary for the controller to fulfil its legal obligation;
- where the data has been made public by the data subject;
- where it is necessary for the establishment, exercise, or protection of a right;
- where it is necessary for the legitimate interests of the controller, provided that it does not harm the fundamental rights and freedoms of the data subject.[43]

With regard to special categories of personal data, Article 6 of the KVKK stipulates that, for data other than those concerning health and sexual life, processing is permitted only where it is expressly provided for by law; whereas data relating to health and sexual life may be pro-

[43] Türkiye, *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, Resmî Gazete, 7 Nisan 2016, m. 5.

cessed solely in limited circumstances such as the protection of public health or for purposes of medical diagnosis and treatment.[44]

In the European Union GDPR, the conditions for processing personal data are set out in Article 6. According to the GDPR, data processing is lawful only if at least one of the following legal bases applies:

- obtaining the data subject's consent;
- the performance of a contract to which the data subject is a party or the taking of steps at the request of the data subject prior to entering into a contract;
- compliance with a legal obligation to which the controller is subject;
- the protection of the vital interests of the data subject or of another natural person;
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- the legitimate interests pursued by the controller or by a third party, provided that such interests are not overridden by the fundamental rights and freedoms of the data subject.[45]

The GDPR also establishes a separate protection regime for "special categories of personal data" under Article 9. In terms of cross border data transfers, both regulations recognise the data subject's consent as an important legal basis. Pursuant to Article 9 of the KVKK, personal data may not be transferred abroad without the explicit consent of the data subject. However, no additional authorization is required for transfers to countries included in the list of countries deemed to provide adequate protection. Transfers to countries lacking adequate protection are permissible only with the explicit consent of the data subject or if the data controllers in Türkiye and in the relevant foreign country provide a written undertaking to ensure adequate protection and obtain authorization from the Personal Data Protection Board.[46]

In the GDPR, cross border data transfers (transfer to third countries) are regulated under Articles 45–49. Transfers to countries with an adequacy decision are permitted without restriction. For transfers to countries without an adequacy decision, appropriate safeguards such as standard contractual clauses or binding corporate rules must be im-

---

[44] *Ibid*., m. 6.

[45] General Data Protection Regulation, art. 6.

[46] KVKK, m. 9.

plemented. Pursuant to Article 49(1)(a) of the GDPR, the informed explicit consent of the data subject constitutes a legal basis for the transfer of data to a third country, even in the absence of an adequacy decision or appropriate safeguards.[47] However, the GDPR treats this consent basis as an exceptional legal ground and emphasizes that, for "continuous and systematic crossborder data transfers," consent alone may not be sufficient, and that such transfers should be carried out on the basis of consent only in exceptional and limited circumstances.[48] Therefore, while the data subject's consent constitutes a legal basis for cross border data transfers under both the KVKK and the GDPR, in the GDPR this basis is regulated as limited and exceptional, whereas under the KVKK consent is recognised as a valid legal ground on its own even for transfers to countries lacking adequate protection. This difference is an important detail that should be taken into account in Türkiye's alignment process with EU data protection standards.

III. Rights of Data Subjects and Obligations of Data Controllers: KVKK–GDPR Comparison

Regulations on the protection of personal data play a critical role in safeguarding individuals' fundamental rights and freedoms in both the Turkish and European Union legal systems. However, in the present study, the rights of data subjects have not been addressed in a comprehensive manner under either KVKK or the European Union's GDPR. The rights regulated under Article 11 of the KVKK and Articles 12–23 of the GDPR differ significantly in terms of scope, exercise procedures, and exceptions.

Data protection law not only sets technical and legal standards for the processing of personal data, but also aims to establish a balance between the rights granted to data subjects and the obligations imposed on data controllers. This balance is essential to ensure that, while protecting individuals' privacy, data processing activities are carried out transparently, accountably, and in compliance with the law.

---

[47] General Data Protection Regulation, art. 49(1)(a).

[48] European Data Protection Board (EDPB), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018.

Under Law No. 6698 on the Protection of Personal Data , the rights granted to data subjects are primarily regulated in Article 11 and include the right to learn whether personal data is being processed; to request information if it has been processed; to learn the purpose of processing and whether the data is used in accordance with that purpose; to know the third parties to whom the data is transferred; to request the correction of incomplete or inaccurate data; to request the deletion or destruction of data pursuant to Article 7 of the KVKK; to object to the emergence of a result against the data subject through the exclusive analysis of data by automated systems; and to demand compensation for damages arising from unlawful data processing.[49] By contrast, under the European Union's GDPR, the rights of data subjects are regulated in a broader and more detailed manner, encompassing rights such as the right to be informed, the right of access, the right to rectification, the right to erasure – the "right to be forgotten," the right to restriction of processing, the right to data portability, the right to object to processing, and the right to be protected against decisions based solely on automated processing.[50] In particular, the rights to "data portability" and "protection against automated processing" are seen as innovative tools that strengthen individuals' effective control over their data in the digital economy.

Table 3. Comparison of Data Subject Rights and Data Controller Obligations under KVKK and GDPR

Aspect	KVKK	GDPR	Key Differences
Material Scope	Art. 2 – Applies to personal data processing by natural/legal persons fully or partially by automated means, and non-automated means if part of a data filing system.	Art. 2 – Applies to processing of personal data wholly or partly by automated means, and non-automated processing if part of a filing system.	Largely similar; GDPR explicitly excludes law enforcement (covered by Directive 2016/680).

[49] Türkiye, *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, Resmî Gazete, 7 Nisan 2016, m. 11.

[50] General Data Protection Regulation, art. 12–23.

Table 3. Comparison of Data Subject Rights

Aspect	KVKK	GDPR	Key Differences
Territorial Scope	Art. 3 – Applies to processing activities of controllers established in Türkiye.	Art. 3 – Applies to controllers/processors in the EU and to non-EU entities offering goods/services to or monitoring individuals in the EU.	GDPR has extra-territorial reach; KVKK does not explicitly.
Data Subject Rights	Art. 11 – Right to learn if data is processed; request information; learn purpose; know recipients; request correction; request deletion/destruction (Art. 7); object to automated decisions; claim damages.	Arts 12–23 – All KVKK rights plus right to be informed (Art. 13–14), right to restriction (Art. 18), right to portability (Art. 20), enhanced safeguards on automated decisions (Art. 22).	GDPR grants broader rights (portability, restriction, enhanced automated decision safeguards).
Obligation: Information	Art. 10 – Obligation to inform data subjects of processing.	Arts 12–14 – Detailed layered privacy notices required.	GDPR is more prescriptive on notice content and format.
Obligation: Data Security	Art. 12 – Take technical/organizational measures to prevent unlawful processing, access, disclosure, alteration, destruction.	Art. 32 – Similar security obligations, but GDPR explicitly includes risk assessment and encryption/pseudonymization.	GDPR includes more explicit technical measures and risk-based approach.
Accountability	Implicit via general obligations.	Art. 5(2) – Controllers must demonstrate compliance.	GDPR's accountability principle is explicit and enforceable.
Breach Notification	No fixed time frame; must inform data subject and Authority without delay if rights are violated.	Arts 33–34 – Notify authority within 72 hours; in some cases inform data subjects.	GDPR has strict deadlines and structured breach reporting.

Table 3. Comparison of Data Subject Rights

Aspect	KVKK	GDPR	Key Differences
DPO Requirement	No explicit requirement.	Arts 37–39 – Mandatory for certain controllers/processors.	GDPR imposes clear DPO obligations.
Record Keeping	VERBIS registration required for certain controllers.	Art. 30 – Maintain detailed records of processing activities.	GDPR's record keeping is broader; KVKK focuses on registry.
International Data Transfers	Art. 9 – Adequacy decision or Board approval; otherwise appropriate safeguards.	Arts 44–50 – Adequacy decision or safeguards (SCCs, BCRs, etc.).	Very similar post-2024 amendment; GDPR has more established mechanisms.
Sanctions	Administrative fines, possible criminal sanctions; amounts generally lower than GDPR.	Art. 83 – Fines up to €20 million or 4% of global annual turnover.	GDPR's sanctions are more severe and proportionate to turnover.[51]

In terms of the obligations of data controllers, there are also significant differences between the KVKK and the GDPR. Pursuant to Articles 10 and 12 of the KVKK, data controllers are obliged to inform the data subject about the data processing activity, take the necessary technical and administrative measures to prevent unlawful processing and access to the data, ensure the exercise of data subjects' rights, and, for those meeting certain criteria, register with the Data Controllers' Registry Information System (VERBIS).[52] The GDPR, on the other hand, imposes a much more comprehensive set of obligations on data controllers. These include, in accordance with the principle of "accountability," ensuring compliance and documenting it at every stage of the data processing cycle; conducting data protection impact assessments for highrisk processing activities; notifying the supervisory authority of data breaches within 72 hours and informing the data subject; entering into writ-

[51] General Data Protection Regulation, art. 2–3, 5(2), 12–23, 28, 30, 32–34, 37–39, 44–50, 83.- KVKK, Arts 2–3, 7, 9–12, 14, 28.

[52] KVKK, m. 10, m. 12.

ten contracts with data processors; and appointing a data protection officer in organizations of a certain scale. [53] This comparison reveals that, in terms of fundamental rights and obligations, the KVKK offers a narrower scope than the GDPR. In particular, the absence in the KVKK of concepts such as "data portability" and "accountability," which are enshrined in the GDPR, demonstrates key areas that Türkiye must address in its process of aligning with EU data protection standards. Therefore, it is considered necessary for the article's title to clearly indicate that it focuses on specific aspects, and for the rights of data subjects and the obligations of data controllers to be examined in a comprehensive manner, as this is essential for both legislative harmonization and comparative legal analysis.

1. Comparison of EU Cyber Security Regulations and KVKK: Recommendations for Türkiye

The acceleration of digitalization and the widespread sharing of data has led to an increase in cyber threats and made the protection of personal data even more critical. The proliferation of digital services and online activities has led to the diversification of cyber threats and increased the need for strong cyber security regulations at national and international level. In this context, the NIS 2 Directive developed by the European Union (EU) provides a comprehensive cyber security framework to ensure the security of digital infrastructures. This directive, which introduces important regulations especially for the protection of critical infrastructures, is of great importance in terms of managing the risks brought by the digitalization process. The European Union implemented important regulations such as the Cyber Resilience Act and the European Cybersecurity Certification Scheme (ECCS) in 2023 to ensure security in the digital world. The Cyber Resilience Act introduces various obligations for manufacturers and importers of digital products. These obligations include conducting risk assessments, providing protection against known vulnerabilities and reporting these vulnerabilities to the national cyber security authority.

---

[53] General Data Protection Regulation, art. 24–39.

KVKK in Türkiye stands out as an important regulation for the protection of personal data. However, the PDPL offers a more limited regulation in terms of scope compared to NIS 2. While the NIS 2 Directive focuses on the security of digital service providers and critical infrastructures, it includes comprehensive regulations such as cyber security risk management, incident reporting and supply chain security. KVKK, on the other hand, focuses more on the processing and protection of personal data. Therefore, to strengthen Türkiye's data security infrastructure, it would be beneficial to integrate some of the articles in NIS 2 into the PDPL. The applicability of NIS 2 in Türkiye and its aligning with the PDPL offers a great opportunity to enhance digital security. Its obligations on cybersecurity risk management, incident reporting, and supply chain security for critical service providers aim to create more secure digital infrastructures across the EU. However, the PDPL needs more comprehensive regulations in these areas. With cyber threats becoming increasingly sophisticated, strengthening Türkiye's data protection and cyber security infrastructure plays a critical role in the digital transformation process. The aligning of the LPPD with NIS 2 will allow Türkiye to raise its data security standards to the EU level through regulations in areas such as cybersecurity risk management, incident reporting, and the responsibilities of managers. This, in turn, will contribute to Türkiye's building a more resilient digital infrastructure against new risks emerging in the digitalization process and will significantly strengthen the country's cyber security strategy. During 2023, significant data breaches in Europe and Ireland provided important lessons for Türkiye. In December 2019, a ransomware attack on Centric Health encrypted the data of 70,000 patients and permanently deleted the data of 2,500 patients. This incident highlights the importance of strong cyber security measures and business continuity plans. Similarly, in May 2023, an attack on the file transfer tool MOVEit resulted in the theft of data of approximately 90 million people. It is also stated that generative artificial intelligence may lead to security vulnerabilities, and threats such as data poisoning may be encountered. Against these risks, it is necessary to implement effective security protocols, train employees, and comply with regulations such as GDPR.[54]

---

[54] Mason Hayes & Curran LLP, *Annual Financial Statements 2024*, https://www.mhc.ie/latest/insights/wrc-2024-annual-report-round-up, [last accessed 6 August 2025].

Legal developments in the European Union and Ireland are important references for Türkiye. For example, the NIS2 Directive has been extended to cover more sectors such as energy and financial services, and member states are required to incorporate this directive into national legislation by October 2024. Failure to comply could result in fines of up to 2% of annual global turnover or €10 million. Similarly, the Cyber Resilience Act focuses on the lifecycle of digital products, while DORA introduces regulations on IT security and resilience testing for financial institutions. The deadline for compliance with DORA is set for January 2025. In addition, amendments to the Cybersecurity Law aim to protect service quality by introducing certification requirements for managed security services. These legislative amendments provide critical lessons for Türkiye to strengthen its cybersecurity strategies and align with global standards. By the introduction of similar regulations in Türkiye, critical infrastructure operators and digital service providers should be required to take certain security measures. ECCS is defined as a voluntary certification scheme under the EU's Cyber Security Act. ECCS sets security standards for information technology products and requires the reporting of vulnerabilities. In addition, national cyber security authorities must sample at least 5 per cent of certified products annually. This structure can also be a source of inspiration for Türkiye. The establishment of voluntary cybersecurity certification programmes in Türkiye could help digital product and service providers to certify their compliance with international standards and increase user confidence.[55] KVKK guarantees the rights of data subjects and imposes obligations on data processors to ensure data security. While the LPPD grants data subjects the rights to be informed, and to access, rectification, erasure, and objection, data processors are obliged to ensure data security and report violations to the Personal Data Protection Authority. However, the PDPL should not be limited to data security, but should also cover the security of digital products. Similarly to the EU's Cyber Resilience Act, Türkiye should make it mandatory for digital product and service providers to comply with certain security standards and report security vulnerabilities. Türkiye can take im-

[55] European Commission, *Cyber Resilience Act – Questions and Answers*, 1 December 2023, Brussels, available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375 [last accessed 6 August 2025].

portant steps in protecting digital infrastructures and personal data by aligning its cybersecurity regulations with existing EU laws. The scope of the LPPD should be expanded so that it is not limited to the protection of personal data, but also covers the security of digital products. Security standards should be set for digital products and manufacturers should be obliged to report security vulnerabilities. These steps will contribute to enhancing digital security in Türkiye.

Türkiye could also develop voluntary cyber security certification schemes similar to the EU's ECCS programme. Such programmes certify the conformity of products and services to international standards and increase user confidence, as well as making Türkiye's digital products more competitive in international markets. The establishment of a national cyber security authority is also important for Türkiye. By expanding the powers and responsibilities of KVKK, this authority can oversee the implementation of cybersecurity standards, identify violations and impose the necessary sanctions. A strong cybersecurity authority will increase the effectiveness of Türkiye's cybersecurity standards and strengthen national security. Finally, national education and awareness raising campaigns should be organized to raise cyber security awareness. These campaigns will enable individuals and organizations to be more prepared against cyber threats and raise the level of cyber security awareness. All actors in the public and private sectors should be encouraged to receive cyber security training. Such trainings will contribute to creating a more secure environment in Türkiye's digital transformation process. Türkiye should expand and strengthen its own legal framework inspired by the EU's cyber security regulations. This will contribute to creating a safer environment for Türkiye's digital transformation process by ensuring both the protection of personal data and the security of digital infrastructures. The EU's regulations such as the Cyber Resilience Act, ECCS and NIS2 Directive can be modelled to strengthen Türkiye's cyber security structure. These regulations will enhance digital security in Türkiye and ensure a stronger stance against global cyber threats.

Conclusions

Law No. 6698 on the KVKK, which is Türkiye's basic law on the protection of personal data, has been an important regulation on data security in the digital world since it entered into force in 2016. This law is based on the European Union's Data Protection Directive 95/46/EC. This Directive aimed to standardize data protection practices among EU countries and ensure the security of personal data. However, shortly after the KVKK entered into force, in 2018, the EU Data Protection Directive was replaced by the GDPR. While the GDPR introduced more comprehensive regulations in terms of data protection, it has had a global impact. Companies operating within the EU or processing EU citizens' data must comply with the GDPR, wherever they are located. This has caused international companies in particular to reconsider their data processing processes. Following the entry into force of the GDPR, the amendments made to the LPPD in 2024 aim to align Türkiye's data protection laws with the GDPR. There are significant similarities between both regulations, especially in data processing, storage, transfer, and security. Both the GDPR and the LPPD require explicit consent for the processing of personal data. In addition, the amendments made to the LPPD in 2024 introduced important regulations in terms of sanctions and penalties to be applied in cases of data breach. The GDPR and the LPPD show significant similarities, especially in the processing of special categories of personal data. The processing of sensitive data such as biometric data, health information, and religious beliefs is subject to the explicit consent of the data subject under both regulations. However, in exceptional cases such as public health, the processing of these data may be permitted. The 2024 amendments to the LPPD in Türkiye have regulated this process in more detail as in the GDPR. Data transfer abroad is strictly regulated by both GDPR and KVKK. According to the GDPR, data transfers outside the EU depend on whether these countries have an adequate level of data protection. With the amendments made in Türkiye, the LPPD has adopted a similar approach to data transfers abroad. Turkish companies will look at the adequacy decision when transferring data abroad and will take certain security measures when transferring data to countries that do not comply with this decision. One

of the most striking features of the GDPR is the harshness of the administrative sanctions imposed against data breaches. In the event of a data breach under the GDPR, companies may be fined up to 4% of their annual revenue. The 2024 amendments to the LPPD increased the fines in this sense, but left them at lower levels compared to the GDPR. These amendments aim to create a stronger deterrence against data breaches in Türkiye. The aligning of the PDPL with the GDPR constitutes an important step in Türkiye's international trade and business relations. Turkish companies that share data with the EU must fully comply with the GDPR. Therefore, these new regulations will accelerate Türkiye's adaptation to global data protection regulations and increase its competitiveness in international markets.

The 2024 amendments to the PDPL are part of Türkiye's efforts to align with global data protection standards. In today's world where digitalization is accelerating, data security has become of critical importance for both individuals and companies. Türkiye's aligning process with the GDPR will increase the country's capacity to respond faster to global developments in the field of data protection and provide higher standards in data security.