www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:5 Sayı:2

Geliş:18.12.2023
Kabul:25.12.2023

Avrupa Birliği ve Türkiye Kişisel Verilerin Korunması Kanunlarının Karşılaştırmalı Analizi: Temel İlkeler, Yasal Dayanaklar ve İlgili Kişi Hakları

Adife Gül, EVREN
Avukat, Konak/İZMİR
av.adifegulevren@gmail.com
ORCID ID: 0009-0008-4205-7538

ÖZ

Bu çalışma, Avrupa Genel Veri Koruma Tüzüğü (GDPR) ve Türk Kişisel Verilerin Korunması Kanunu'nun (KVKK) veri işlemeye halim olan temel ilkeler, özel nitelikli kişisel veriler için belirlenenler dahil olmak üzere temel veri işleme şartları ve veri sahiplerinin hakları yönünden benzerlik ve farklılıklarına odaklanarak kısa bir inceleme gerçekleştirmektedir. Temel ilkelerde iki düzenleme arasında önemli bir uyumun varlığı sergilenirken, özellikle bazı veri işleme şartları ve ilgili tarafların haklarına odaklanan düzenlemelerde farklılar üzerinde durulmaktadır. Bununla beraber, iki mevzuat arasında gözlemlenen uyumluluğun aynı zamanda Türkiye Kişisel Verileri Koruma Kurumu'nun proaktif çabalarına dayandığı belirtilmektedir. Son olarak, her ne kadar iki mevzuat arasında farklılıklar bulunsa da, bu çalışma, Türk yetkililerin GDPR ile tam uyumluluğu sağlama konusundaki kararlılığını vurgulayarak bütünsel bir yaklaşımla tam uyumun sağlanabileceğini ifade eder.
Anahtar Sözcükler: KVKK, GDPR, kişisel verilerin korunması, temel ilkeler, veri işleme şartları, ilgili kişi hakları, karşılaştırmalı analiz

A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects

ABSTRACT

This study provides a brief overview of the European General Data Protection Regulation (GDPR) and the Turkish Personal Data Protection Law (KVKK), specifically examining their similarities and differences in terms of fundamental principles governing data processing, legal grounds for personal data processing, including for processing special categories of personal data, and the rights of data subjects. While a significant alignment is observed between the two regulations regarding fundamental principles, the study highlights differences, particularly in certain data processing conditions and regulations pertaining to the rights of relevant parties. It is noted that the coherence observed between the two legislations is also attributed to the proactive efforts of the Turkish Personal Data Protection Authority. In conclusion, despite disparities between the two legislations, the study underscores the commitment of Turkish authorities to ensure full compliance with the GDPR and asserts that comprehensive compliance can be attained through a holistic approach.
Anahtar Sözcükler: KVKK, GDPR, personal data protection, legal principles, legal grounds, data subjects rights, comparative analysis.

Atıf Gösterme	Evren, A. G., (2023). Avrupa Birliği ve Türkiye Kişisel Verilerin Korunması Kanunlarının Karşılaştırmalı Analizi: Temel İlkeler, Yasal Dayanaklar ve İlgili Kişi Hakları, *Kişisel Verileri Koruma Dergisi. 5*(2), 39-64.

INTRODUCTION

As technology advances, public authorities grapple with the challenge of balancing human rights and technological use. While digital systems offer practical benefits, they can also pose risks to human rights, particularly in the realm of personal data privacy. The protection of personal data has become a global priority, given its crucial role in nearly every business sector. The European Union (EU) plays an essential role as one of the main regulators that support technological developments while equally protecting fundamental human rights. While shaping the European digital future, the European Commission formulates one of the most important regulations; the General Data Protection Regulation. ("GDPR") (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, And Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1)

The GDPR provides important protection for personal data and sets certain rules for processing personal data. Since EU regulations are binding for all member states, it follows that data protection rules under the GDPR should be adhered to by all EU members. However, the impact of the GDPR extends beyond EU member states to include Turkey. Despite not being an EU member, Turkey, as a developing country geographically close to Europe, aspires to achieve a high level of human rights protection and democracy (Presidency of Republic of Turkey Presidency of Strategy and Budget, 2019, p.2 para. 5). While Turkey's accession negotiations with the EU have stalled, EU legislation has consistently served as a source of inspiration.

The Turkish Personal Data Protection Act No: 6698 ("KVKK") was legislated with the inspiration of the EU Directive 95/46/EC, as the GDPR had not yet entered into force during the preparation process ("Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu | Kişisel Verileri Koruma Kurumu", 2019, pp. 32, 75, 77) Although the GDPR was not the direct basis for the KVKK, the Turkish Personal Data Protection Authority ("Authority") has consistently aligned its decisions and guidelines with the GDPR's essence. In summary, the KVKK was ratified on April 14, 2016, and came into force on May 5, 2018. Through secondary legislations, it aims to provide an equivalent level of protection to data subjects in personal data processing activities as the GDPR. Turkey has publicly announced its goal to revise the KVKK by 2023, ensuring full compatibility with the GDPR. (refer to "The Eleventh Development Plan | Presidency of Republic of Turkey Presidency of Strategy and Budget", 2019, p.121 para 479.1)

This essay aims to evaluate the current alignment of the KVKK and the GDPR concerning fundamental principles, legal foundations, and the rights of data subjects. The analysis delves into each principle, legal ground, and data subject right in a comparative manner, shedding light on both commonalities and differences between the two regulations on specific subjects. Additionally, it examines how these variations may influence the implementation of data protection rules and impact data subjects

In summary, the essay contends that, despite some disparities between the KVKK and GDPR, they demonstrate substantial compatibility concerning key principles of personal data protection. However, alongside their similarities, notable distinctions exist, particularly in the regulation of specific legal grounds and the definition of data subject rights. The essay argues that this compatibility is mainly attributed to the proactive efforts and publications of the Authority, rather than inherent provisions

within the KVKK, given its comparatively less detailed nature and gaps in addressing certain issues. Nevertheless, through a comprehensive approach and meticulous amendments, the KVKK has the potential to attain an equivalent level of protection as the GDPR, particularly concerning fundamental principles, legal grounds, and data subjects' rights.

LEGAL PRINCIPLES

The legal principles that govern personal data processing operations constitute a critical set of rules, establishing the primary guidelines for every processing activity. These principles are formulated in both the GDPR and the KVKK with the aim of safeguarding individuals' rights (Van Alsenoy, 2019, para 47) and providing a framework for the responsible and ethical handling of personal data. ("Temel İlkeler | Kişisel Verileri Koruma Kurumu", n.d., p.1) Given that some of these principles serve as a foundation for more detailed provisions (Europe & Rights, 2018, p.116), it is crucial to have a clear understanding of each principle and its significance. To conduct a comparative analysis, the legal principles outlined in the GDPR and KVKK are delineated below shortly:

i. Lawfulness; Processing activities must be founded on at least one legal ground.

- Art. 5(1)(a) of the GDPR, Art. 4(2)(a) of the KVKK

ii. Fairness; This principle encompasses data subjects' positive expectations regarding processing activities or their awareness of the processing, especially when the processing is legally permitted to occur by a law. Furthermore, fairness involves conducting a just assessment of processing activities; if the processing negatively impacts data subjects, it would be considered unfair.

- Art. 5(1)(a) of the GDPR, Art. 4(2)(a) of the KVKK

iii. Transparency; Processing activities should be conducted in a transparent and open manner by effectively informing data subjects.

- Art. 5(1)(a) of the GDPR, although missing in the KVKK, these principles are found in the guidelines and decisions of the Authority. Moreover, the transparency principle should be construed as an extension of the fairness principle. (Develioğlu, 2017, s. 45)

iv. Accountability; Controllers are obligated to demonstrate and furnish proof of compliance with the GDPR and KVKK for all processing activities.

- Art. 5(2) of the GDPR, although missing in the KVKK, these principles are found in the guidelines and decisions of the Authority. Moreover, while accountability is considered a principle in the GDPR, it is, in fact, more of a responsibility for the controller (Besemer, 2020, p.96). From this perspective, the accountability principle aligns with the spirit of the KVKK, if not its explicit language (Kaya, 2021, p.1895). The KVKK and its secondary legislations impose certain obligations on controllers, validating the accountability principle. These obligations include the requirement to register with the Register of Controllers, maintain an inventory, publish a personal data retention and destruction policy, and establish a policy regarding special categories of personal data (Kaya, 2021). In the GDPR, we see the concepts; data protection officer (Art.37), records of processing (Art.30), data protection impact assessment (Art.35), prior consultation (Art.36), codes of conducts (Art.40), certification (Art.42), the legal binding of processors (Art. 28(3)), co-operation with supervisory authorities (Art. 31), personal data breach notification (Arts. 33–34) as accountability tools. (Van Alsenoy, 2019, p.44, para 68)

Despite variations in the obligations imposed on controllers by these regulations, it is evident that both frameworks emphasize the importance of accountability.

i. Purpose Limitation; Controllers must confine the utilization of processed personal data to the intended legitimate purpose of processing.

- Art. 5(1)(b) of the GDPR, Art. 4(2)(c) of the KVKK

ii. Data Minimization; Controllers should only process the minimal and relevant personal data necessary to achieve their intended purpose. This emphasizes the requirement for personal data processing to be both necessary and proportional to the specified purpose.

- Art. 5(1)(c) of the GDPR, Art. 4(2)(ç) of the KVKK

iii. Accuracy; Controllers are obliged to ensure the correctness and currency of the personal data they process.

- Art. 5(1)(d) of the GDPR, Art. 4(2)(f) of the KVKK

iv. Storage Limitation; Personal data of data subjects should be stored only for as long as necessary for processing purposes.

- Art. 5(1)(e) of the GDPR, Art. 4(2)(d) of the KVKK

v. Integrity and Confidentiality; Controllers are required to exert efforts to ensure the security and integrity of their personal data, both technically and operationally.

- Art. 5(1)(f) of the GDPR, although missing in the KVKK, these principles are validated under the scope of Art. 12 of the KVKK.

In the comparative analysis, it is observed that the enumerated principles are identical, but some are not explicitly stated in the KVKK. Concerning the principles of transparency and accountability, even though they are not expressly mentioned under the title of 'Legal Principles,' we see references to these principles in various decisions and guidelines of the Authority. (see "2019/125 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurulu", 2019; "The Criteria for The Determination of Countries Having an Adequate Level of Protection | Kişisel Verileri Koruma Kurulu", 2019, p.1 para. 8; "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler| Kişisel Verileri Koruma Kurulu", n.d., p.16) Moreover, transparency in the KVKK can be considered an integral aspect of fairness principles, and accountability is demonstrated through the obligation of controllers to comply with the KVKK. Additionally, Art. 12 of the KVKK addresses the absent principles of integrity and confidentiality by mandating controllers to implement necessary measures to ensure the security of personal data.
Another distinction is that the GDPR elaborates on principles before naming them, whereas the KVKK presents a list of named principles. The explanatory aspect of the principles is covered in the Authority's Guideline regarding Basic Principles. Hence, the comparison above is conducted by assessing the KVKK and the Authority's Guidelines. Consequently, due to the substantial contribution of the Authority and the interpretation of the KVKK, not only for principles but also holistically, the legal principles of the GDPR and the KVKK demonstrate compatibility. Where a legal principle is referenced under the GDPR, the same interpretation applies under the KVKK.

LEGAL GROUNDS

Legal bases play a crucial role in providing a framework for controllers and guiding decisions on the lawfulness and fairness of data processing activities (Rücker & Kugler, 2017, para 359). Essentially, legal bases act as a map for controllers, aiding them in determining the justifications for processing. A clear identification of legal grounds for each processing activity is crucial for data subjects, as the exercise of some data subject rights is linked to specific legal grounds. Both the GDPR and the KVKK provide various legal bases to controllers for processing activities. The following comparative analysis outlines the legal bases of both the KVKK and the GDPR:

- **Consent;** Refers to a freely given, specific, informed, and unambiguous indication, whether by a statement or clear affirmative action, signifying agreement to the processing of personal data by a data subject.

    - Art. 6(1)(a) of the GDPR, Art. 5(1) of the KVKK

The KVKK, in regulating the legal bases for processing personal data, adopts a different approach from the GDPR. According to the explicit provision in Article 5(1) of the KVKK, personal data cannot be processed without the explicit consent of the data subject as a general rule. Initially, this led to the understanding that consent is the primary legal basis, and the others are applicable only if consent is not obtained (Han, 2019). Consequently, data controllers in Turkey have attempted to obtain consent for every processing activity, resulting in chaos in practice. However, the Authority intervened, clarifying that if other legal bases, as outlined in Art. 5(2) of the KVKK, are available for a processing activity, obtaining consent is not mandatory. (see "Doğru Bilinen Yanlışlar 2 | Kişisel Verileri Koruma Kurumu", n.d, p.15; "Sıkça Sorulan Sorular | Kişisel Verileri Koruma Kurumu", 2019, p.24; Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu, n.d. pp. 2-3). Asking for consent when other legal bases exist was deemed misleading and not a lawful form of consent. Consequently, the Authority declared that consent is not the primary basis for processing personal data in the KVKK; rather, it is one of several legal bases, aligning with the GDPR. Despite no amendments to the KVKK, the Authority's consistent reminders have prompted adjustments in practice. In a notable example, decision number 2020/173 regarding Amazon Turkey emphasized, "Taking explicit consent in the presence of processing reasons other than explicit consent is interpreted as a violation of the rule of good faith." ("2020/173 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurumu", 2020)

A notable distinction regarding consent is that while the GDPR has a separate provision, Art.7, regulating conditions for consent, the KVKK lacks additional provision for conditions. However, the Authority addresses this by providing guidelines and communiqués, ensuring that the conditions for consent sought for processing in Turkey align with those sought under the GDPR (see "Communique on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform | Kişisel Verileri Koruma Kurumu", 2018, Art.5(1)(a), Art. 5(1)(f); "Açık Rıza | Kişisel Verileri Koruma Kurumu", n.d.) Please refer to Table 1 below for a comparative analysis of the conditions for consent under both regulations.

Table1
Conditions of Consent Comparatively

Conditions of Consent	GDPR	KVKK

Disclosure of processing purposes requiring consent is necessary	Art.(6)(1)(a)	Authority's Consent Guideline p.4
Controllers bear the burden of proof	Art.7(1)	Authority's Consent Guideline p.3
A distinct and separate approach is necessary when seeking consent alongside other matters in writing	Art.7(2)	Communique of the Authority on Information Obligation Art.(5)(1)(f) The information obligation must be fulfilled independently of the consent-taking process
Consent sought in writing must be presented in an intelligible and easily accessible form, using clear and plain language	Art.7(2)	Authority's Consent Guideline p.5
Controllers have an information obligation before soliciting consent	Art. 7(3)	Communique of the Authority Art.(5)(1)(a), Authority, Consent Guideline p.5
Providing individuals with a genuine opportunity to refuse being subjected to processing requires consent	Art.7(3)	Authority's Consent Guideline p.6
Offering an effective and user-friendly withdrawal mechanism is mandatory	Art.7(3)	Authority's Guideline-True Known Faults 2 pp.17-18
Consent cannot be made conditional on the provision of services for being able to process personal data not necessary for the performance of the contract	Art. 7(4)	Authority's Consent Guideline, p.6
if adverse consequences may arise as a result of processing, then the consent cannot be considered freely given and therefore not valid	European Data Protection Board ("EDPB") Guidelines 05/2020 para 22	Authority's Consent Guideline, p.6
if there is a clear imbalance of power in the relationship between the controller and the data subject, the validity of the explicit consent of data subjects may be suspect	EDPB Guidelines 05/2020, para 21	Authority's Consent Guideline, p.6

In the realm of KVKK implementation, specifically concerning consent, the Authority has elucidated essential conditions. Three pivotal points are underscored by the Authority: consent should be grounded in free will and prior information, and it should be granted for a specific processing activity ("Açık Rıza | Kişisel Verileri Koruma Kurumu"). Notably, the condition that consent should be based on "free will" encompasses most scenarios that cast doubt on the validity of consent highlighted by the EDPB guidelines. For example, consent may be deemed suspect in cases of power imbalances or potential adverse consequences, as these situations pose questions about the genuine essence of free will.

The other distinction regarding consent lies in the absence of a specific provision within the KVKK, unlike the GDPR, which addresses consent for children concerning information society services through Article 8. Consequently, regarding child consent for information society services in Turkey, there is no prescribed age limit to establish the validity of consent. This implies that, in every case, a separate examination is required to determine the validity of child consent, adhering to both personal data protection regulations and other applicable related laws. (Uçak, M., 2021, p.58)

Finally, the GDPR offers supplementary provisions when the legal basis is consent, aiming to balance the rights of data subjects and controllers. These provisions are not expressly included in the KVKK. Here is the list of them:

- Information about the right to withdraw consent at any time (Art. 13(2)(c), Art. 14(2)(d))
- Right to erasure (Art. 17(1)(b))
- Notification obligation regarding erasure (Art. 19)
- Right to data portability (Art. 20)

While there is no specific provision addressing the issues mentioned above in the KVKK, with the exception of the right to data portability, the others are covered. The Authority acknowledges the right to withdraw consent at any time (refer to "Açık Rıza Alırken Dikkat Edilecek Hususlar | Kişisel Verileri Koruma Kurumu", n.d) therefore, this information is typically provided in practice in asking consent. On the other hand, the right to erasure is recognized under Art. 11(e) of the KVKK, granting data subjects the right to request erasure if the conditions outlined in Art. 7 are met. According to Art. 7, if the reasons for processing no longer exist, data subjects have the right to erasure. This implies that if consent is withdrawn, and there is no other available basis, a controller is obligated to erase personal data upon the data subject's request. Additionally, Art. 11(f) allows data subjects to request notification to third parties about the erasure. Consequently, once more, considering the Authority's Guidelines and other provisions of the KVKK, the KVKK addresses the previously mentioned missing points, except for the right to data portability.

i. **Performance of a contract, taking necessary steps to enter into a contract at the request of a data subject;** Refers to a situation processing personal data should be required for the execution of a contractual agreement or establishment of a contract with the data subject.

- Art. 6(1)(b) of the GDPR, Art. 5(2)(c) of the KVKK

Article 6(1)(b) of the GDPR lacks a precise definition of "performance of a contract," with Recital 44 merely indicating that processing can occur in the context of a contract or with the intention of entering into one. However, additional clarification on the conditions for relying on the performance of a contract is provided by decisions and guidelines from the EDPB, such as EDPB Guidelines 2/2019, EDPB Binding Decision 3/2022. According to these sources, the processing must be objectively necessary for a specific purpose and an integral part of delivering the contracted service to the data subject. Moreover, the EDPB emphasizes the alignment of perspectives on the necessity of processing personal data between controllers and data subjects, as controllers must justify the necessity of personal data through mutual understanding. ("Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR) | European Data Protection Board", n.d., para 113) The same approach can be applicable under the KVKK since the KVKK uses the term "directly related to the establishment or performance of the contract" while explaining this basis under Article 5(2)(c).

In light of this information, under both regulations, the legal basis "performance of a contract" should be narrowly interpreted, referring only to the core obligations outlined in the contract. Processing that is not objectively necessary for fulfilling these obligations, although potentially beneficial for the business or operations of controllers, falls outside the scope of "performance of the contract," as emphasized by the EDPB. (Binding Decision 3/2022, paras 120-121) Failure to do so would undermine

the rights of data subjects, as the legal basis for processing would not rely on consent or legitimate interest, both of which demand additional care, such as conducting a balancing test or providing a real opportunity to refuse consent and rights for data subjects (Binding Decision 3/2022, para. 131). Besides, consent or legitimate interests as legal bases also afford greater protection for controllers by providing the right to withdraw consent. (Art. 7(3)), the right to object (Art. 21(1)), and the right to be forgotten (Art. 17(1)(b), Art. 17(1)(c) under the GDPR (Binding Decision 3/2022, para. 131) Although the right to object is not included in the KVKK, it is an undeniable fact that the overly use of the "performance of a contract" would not align with the nature of the KVKK and Article 5(2)(c).

ii. **Legal obligation;** Refers to a legal obligation to be needed fulfill.

- Art. 6(1)(c) of the GDPR, Art. 5(2)(ç) of the KVKK

Both the GDPR and KVKK incorporate the "legal obligation" as a legal ground into their provisions; however, the interpretation of this basis varies between the two regulations. In the context of the GDPR, for processing to be based on this ground, it is necessary to demonstrate that the processing of personal data is essential for compliance with the law (Besemer, 2020, p.132, ch.4.1.2). According to Article 6(3) and Recital 43, "a legal obligation" should serve as a legal basis or legislative measure. Therefore, under the GDPR, a legal obligation cannot derive from a contract or any other legal relationship aside from a law (Ustaran, 2022, p.185, ch.7.2.4).

Under the KVKK as well, a “legal obligation” generally refers to a controller's legal obligation arising from law. (Bilir, 2020, p.325) Therefore, under the KVKK, the bases of "legal obligation" and "expressly provided for by the law" may intersect. However, this legal ground also covers contractual obligations too. (Bilir, 2020, p.325) Thus, when it is not expressly provided by the law—such as when the law implicitly or generally requires personal data processing or a contractual relationship necessitates a personal data process beyond what is needed for the entry or performance of a contract—this basis can be utilized under the KVKK implementation.

Consequently, the legal obligation as a legal ground under the GDPR is essentially identical to the legal ground "expressly provided for by the law" in the KVKK because the scope of the legal obligation under the KVKK is broader, encompassing legal obligations arising from legal relationships too other than law.

iii. **Vital interest;** Refers to a situation that processing personal data is necessary to protect vital interest of data subjects or others like right to live.

- Art. 6(1)(d) of the GDPR, Art. 5(2)(b) of the KVKK

The concept of "vital interest" revolves around circumstances of life or death, as articulated in Recital 46 of the GDPR, and is only applicable when processing cannot manifestly be grounded in another legal basis. Consequently, the scope of applying this legal ground is rather limited in the GDPR. (Dienst, 2017, p. 81, para 386) Nevertheless, vital interest under the KVKK differs slightly, as it permits processing based on this ground if a data subject is unable to express consent, and processing is necessary to safeguard their own or others' life or bodily integrity. Therefore, KVKK's vital interest is applicable only when consent is not feasible. In contrast, GDPR Art. 6(1)(d) does not explicitly confine the use of this legal ground to situations where consent cannot be obtained. Hence, the operational details of the two regulations vary in practice. The KVKK’s implementation on this aligns more with Article 9(2)(c) of the GDPR, which pertains to processing special categories of personal data to protect the vital

interest of data subjects or others if data subjects physically or legally incapable of giving consent. On the other hand, the KVKK allows relying on this basis when a data subject is unable to express consent due to physical disability or a legally invalidated situation. Therefore, it is fair to say that the scope of this basis in the KVKK is broader than a life-death situation as in the GDPR.

iv. **Legitimate interest;** refers to situation that a current and present benefit which is conformable with laws stands for that specific processing. ("Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" | Article 29 Data Protection Working Party", pp.24-25; "Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu", n.d, pp.11-16)

- Art. 6(1)(f) of the GDPR, Art. 5(2)(f) of the KVKK

While other legal bases for processing personal data are self-explanatory (such as a contractual obligation or legal requirement), the legitimate interest provides controllers with a degree of freedom. However, this freedom is not absolute as it is limited by the principles and essence of the GDPR and KVKK. There are some conditions to be relying on this base through the EDPB and the Authority guidelines and decisions. As a result, conducting a balance test is required since under both regulations processing is allowed by relying on this legal basis if the interests or fundamental rights and freedoms of the data subjects are not overridden. (Art.6(1)(f); Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu,p.14)

The balancing test is a meticulous examination that scrutinizes whether the controllers' interests supersede those of the data subjects, considering all facets of the desired processing. This evaluation encompasses both positive and negative aspects associated with processing activities related to legitimate interests, and it delves into the measures implemented to ensure a harmonious balance of interests. In essence, the balancing test serves as a cornerstone for upholding the accountability of controllers, serving as a proof of fair processing practices. Even if the legitimate interests of controllers do not unequivocally outweigh the interests of data subjects, processing based on legitimate interests must be proportionate for it to be deemed lawful, as stipulated in WP29 Opinion 06/2014 (p.11, p.43). This requirement, articulated in the WP29 Opinion 06/2014 (p.11, p.43), holds significant relevance for compliance with the KVKK, as the principles of data minimization, purpose limitation, and fairness necessitate such proportionality. The decisions and guidelines of the Authorities emphasize specific criteria that are instrumental in conducting balancing tests for processing based on legitimate interests, providing a structured framework for this evaluative process. (Please refer to "Opinion 06/2014 on the 'Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' | Article 29 Data Protection Working Party"; "2019/78 Sayılı Karar Özeti | Kişisel Verileri Koruma Kurulu")

When examining two opinions/decisions, a clear distinction emerges: the KVKK decision numbered 2019/78 emphasizes establishing the essential necessity of legitimate interests, while the WP29 provides detailed instructions on conducting a balancing test. Consequently, it is accurate to assert that the KVKK implementation needs to benefit from additional guidance. Furthermore, the absence of the concept of a data protection impact assessment (Art.29 of the GDPR) in the KVKK creates a notable gap. In situations where processing relies on legitimate interests and involves new technologies with the potential for risky outcomes, there is no inherent mechanism compelling a more comprehensive assessment.

On the other hand, due to the inherently risky nature of legitimate interest, the GDPR affords data subjects additional rights under specific conditions and imposes additional obligations on controllers

when the legal basis for processing is legitimate interest. Here are additional provisions concerning legitimate interest that the KVKK does not encompass:

- Obligation to inform data subjects what the legitimate interest relying on the process is, GDPR Art.13(1)(d), Art.14(2)(b)
- Right to object if the legal ground the legitimate interest, GDPR Article 21(1)
- Right to erasure, GDPR Art. 17(1)(c)
- Right to rectification, GDPR Art. 18/(1)(d)
- Notification obligation regarding erasure, Art.19

The GDPR requires controllers to explicitly disclose the specifics of their legitimate interests. However, the KVKK does not impose a similar obligation. This disparity creates a disadvantage for data subjects in exercising control over their personal data. On the other hand, the GDPR's right to erasure concerning legitimate interests is closely tied to the right to object. If a data subject objects to processing based on legitimate interests, the controller must demonstrate that its legitimate grounds outweigh the rights and freedoms of data subjects, or that processing is necessary for the establishment or exercise of legal claims. In cases where the controller fails to demonstrate this, it is obligated to erase the personal data of the data subject upon their request under Art. 17(1)(c) of the GDPR.

Even though the KVKK lacks above mentioned specific provisions, it does not preclude a data subject from objecting to processing based on legitimate interest or requesting the right to erasure. Data subjects can still rely on general terms and claim the unlawfulness of processing based on legitimate interest. If the processing is deemed unlawful, due to lack of reason to process, the controller will be compelled to erase the processed personal data. However, it is undeniable that this approach may require more effort and be more time-consuming for data subjects.

v. Performance of a public interest task or the exercise of official authority;

- Art. 6(1)(e) of the GDPR, Missing in the KVKK

Under GDPR, one of the main legal bases for processing personal data is the public interest or exercising official authority. This means that processing should be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal ground is particularly relevant for public authorities, such as law enforcement agencies or government bodies, who may need to process personal data to carry out their tasks. Besides, it is also applicable to private sectors when a governmental outsource its tasks. (Dienst, 2017, p.81, para 389) The KVKK lacks this legal basis. As a result, public authorities or other outsourced institutions carrying out public tasks have to rely on other available legal bases like “expressly provided by the law” or “legal obligation” or even “legitimate interest” which is prohibited to be relying on by public authorities under the GDPR. (Art.6)

According to the GDPR, the purpose of processing for reasons of public interest/task should be established by law, as specified in Article 6(3) of the GDPR. Hence, in the GDPR implementation, the processing of personal data by public authorities is permissible under the laws. This is similar to the KVKK, as public authorities most of the time should rely on the legal ground "expressly provided by the law" under the KVKK. However, unlike the KVKK, the GDPR emphasizes the quality of the law relied upon for processing for public interest (Art.6(3)(2), which strengthens the rights of data subjects.

On the other hand, similar to being in legitimate interest, if processing is based on public interest, data subjects within the scope of the KVKK lack some additional rights and protections provided by the GDPR. These include the obligation to have a data protection officer in public authorities (Art.37(1)(a)) or the right to object (Art. 21) and the specific version of right to erasure (Art. 17(1)(c)). As explained under the title "legitimate interest," this doesn't result in a complete lack of rights for data subjects. They can still contest the unlawfulness and unreasonableness of the processing. However, if a specific law governs the processing, emphasizing unlawfulness would be less likely, as the KVKK does not underscore the quality of the law that constitutes the basis for public interest, as evident in GDPR Article 6(3)(2).

vi. Expressly provided for by the law

- Missing in the GDPR, Art. 5(2)(a) of the KVKK

Even though it appears to be an additional basis in the KVKK, not included in the GDPR, this basis aligns with the concepts of "legal obligation" and/or "public interest" under the GDPR. The GDPR prefers the term "legal obligation" to signify processing for compliance with the law and "public interest" to indicate processing for an interest laid down by the law. Therefore, given that the details were provided under those titles, there won't be an additional examination here.

vii. Personal data have been made public by the data subject;

- Missing in the GDPR, Art. 5(2)(d) of the KVKK

Personal data made public by the data subject is considered one of the legal bases under the KVKK, setting it apart from the GDPR. In contrast, the GDPR treats the concept of personal data made public by the data subject as an exception to the prohibition of processing special categories of personal data, as outlined in Article 9(2)(e). While personal data made public by the data subject serves as a legal ground under the KVKK, the application of it is not straightforward, as indicated by the decisions of the Authority. The Authority emphasizes a narrow interpretation of personal data that has been publicly made available. ("Alenileştirme" Hakkında Kamuoyu Duyurusu | Kişisel Verileri Koruma Kurumu", 2020) For data to be considered publicly available, it must be evident that the data subject had a clear intention to make their personal data public without reservation. ("Alenileştirme" Hakkında Kamuoyu Duyurusu | Kişisel Verileri Koruma Kurumu", 2020) This stance aligns with the opinion of the Advocate General in C-252/21, asserting that data subjects must be fully aware that they are making their personal data public to benefit from the exception for processing special categories of personal data ("Press Release No 158/22 |Court of Justice of the European Union", 2022).

In conclusion, although personal data being made public is recognized as one of the legal bases in the KVKK, its application is notably limited, reflecting the cautious approach emphasized by both the Authority and legal opinions.

viii. Data processing is necessary for the establishment, exercise or protection of any right;

- Missing in the GDPR, Art. 5(1)(e) of the KVKK

This legal basis under the KVKK provides an opportunity for processing when there is a right stemming from legal, administrative, or any related grounds. ("Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu", p.11) It is commonly employed for processing activities aimed at exercising or defending legal claims and most of controllers keep files of data subject during legal lapse of the time by relying on this basis. ("Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu", p.11)

The GDPR lacks the inclusion of this specific legal basis. Its approach to the concept of establishing, exercising, or defending legal claims diverges significantly, manifesting in two distinctive ways. Firstly, it serves as an exception to the prohibition of processing special categories of personal data, as particularly detailed in Article 9(2)(f). Secondly, it permits the continuation of processing activities even if data subjects exercise their rights to object, erasure, and restriction, as outlined in Articles 17(3)(e), 18(2), and 21(1). Consequently, the GDPR views this concept as an exception related to the exercise of the legal rights of data subjects and the prohibition of processing special categories of personal data.

The GDPR's approach is strategically crafted to enhance data subjects' control over their personal data, as evidenced by the utilization of the right to restriction of processing—a provision conspicuously absent in the KVKK. Under the GDPR, this right can be invoked when there is no necessity for processing personal data but a compelling need for the establishment, exercise, or defense of legal claims. This protective measure safeguards the rights of data subjects, as the restriction of processing entails temporarily relocating the specified data to another processing system, rendering the selected personal data inaccessible to users or temporarily removing published data from a website (refer to Recital 67 of the GDPR).

SPECIAL CATEGORIES OF PERSONAL DATA AND AVAILABLE LEGAL GROUNDS FOR THEM

Special Categories of Personal Data Defined by Regulations

Most of the special categories of personal data align under both the GDPR and the KVKK. These encompass racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, and data concerning a person's sex life. Although the KVKK doesn't explicitly state sexual orientation as a special category of personal data, it can be inferred that this category falls under the broader classification of someone's sex life. While most categories are consistent, the KVKK introduces two additional special categories of personal data.

One of the additional categories in the KVKK is "criminal conviction," which is separately regulated in Article 10 of the GDPR. It specifies that only official authorities and controllers providing appropriate safeguards, authorized specifically by the law, can process personal data related to criminal convictions, offenses, or security measures. If the KVKK were to adopt this approach, it could lead to fairer implementations. Currently, under the KVKK, records such as inhibition or custody are not considered criminal convictions and are not categorized as special personal data since they are preventive measures rather than final verdicts. However, a record related to an ordinary offense constitutes a special category of personal data. Moreover, under the KVKK, controllers that are not judicial institutions, official authorities, or authorized controllers by law can process someone's criminal conviction records with the consent of data subjects, potentially leading to human rights violations in practice.

Another additional special category of personal data in the KVKK is "appearance," encompassing tattoos, clothing preferences, hair and mustache styles, and any other data related to the physical body's reflection. These types of data are considered special categories because they can provide information about someone's religious, political, or philosophical beliefs. However, if the purpose of designating "appearance" as a special category is to prevent discrimination based on one's beliefs, it may not be necessary since religious, political, or philosophical beliefs already constitute special categories of personal data. Therefore, there is no added value in including "appearance" among the special categories of personal data.

Legal Grounds for Processing Special Categories of Personal Data

The conditions for processing special categories of personal data differs between the GDPR and KVKK implementations. Consequently, the evaluation of the lawfulness of such processing and the available legal bases or exceptions will vary between the GDPR and KVKK. Moreover, the GDPR mandates controllers to appoint a data protection officer (DPO) if they are processing special categories of personal data on a large scale. Large-scale processing can be identified by assessing factors such as the volume of data, the number of data subjects, the duration, or the geographical extent of the processing activity (Article 37(1)(c)) (“Guidelines on Data Protection Officers ('DPOs') | Article29 Working Party” , 2017, p.21). If the KVKK encompasses the concept of a DPO similar to the GDPR, a hospital recording patient data, which includes special categories, would be required to appoint a DPO based on this assessment.

In the context of processing special categories of personal data, while the GDPR acknowledges "exceptional" conditions as an exemption to the general prohibition, the KVKK adheres to a framework of "legal bases" similar to the processing of non-special categories of personal data. Art. 9(2) of the GDPR outlines distinct legal exceptions for each category of special personal data. Conversely, the KVKK adopts a more restrictive stance on the processing of special categories of personal data, providing limited bases for such processing. The following table presents a comparative analysis.

Table 2:
Legal Grounds/Exceptions for Processing Special Category Personal Data

Special Category Personal Data Processing Exceptions in the GDPR	**Legal Grounds for Processing Special Categories of Personal Data in the KVKK**
Can be processed if one of the below exceptions exist: · • Explicit Consent, Art. 9(2(a) • Employment and social security and social protection law, Art. 9(2)(b) • Legitimate activities of a foundation, association or any other not-for-profit body • Personal data which are manifestly made	For data concerning health, and data concerning a natural person's sex life; • Explicit consent, Art. (6)(2) • by only persons subject to secrecy obligation or competent public institutions public health protection, preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services, as well as their

public by the data subject, Art. 9(2)(e) · • For reasons of substantial public interest, Art. 9(2)(g) • For the purposes of preventive or occupational medicine, Art. 9(2)(h) • For reasons of public interest in the area of public health 9(2)(i) • For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 9(2)(j)	financing, Art. (6)(3) For other special categories; • Explicit consent Art. (6)(3) • If it is expressly provided for by the laws Art.(6)(3)

Consent is one of the legal bases/exceptions for processing special categories of personal data. However, in addition to consent, the KVKK only allows the processing of special categories of personal data when expressly provided by law, except for health and sexual life. For health and sexual life, the KVKK offers a legal ground identical to that found under Art.9(1)(h) of the GDPR which is for the purposes of preventive or occupational medicine. However, this only legal basis offered by the KVKK for processing health data causes difficulties in practice, particularly for employers.

According to the KVKK, health data can only be processed by persons subject to secrecy obligations or competent public institutions for specific purposes, such as the protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services, and financing. As employers do not identically fall under this exception, they must obtain consent from data subjects. However, according to the Authority guidelines (see "Açık Rıza | Kişisel Verileri Koruma Kurumu", p.7) which are similar to the European Data Protection Board's decisions and guidelines, the validity of consent in employer-employee relationships is suspect. Besides, data subjects have the right to withdraw their consent. Consequently, in practice, it becomes impossible to process health data even though it is a legal obligation for employers to assess the working capacity of the employee and protect the vital interests of other employees.

Finally, Article 9 of the KVKK states that the Authority is empowered to take adequate measures in the processing of special categories of personal data. Consequently, the Authority has outlined a set of measures, such as non-disclosure agreements, determination of access rights, cryptographic retention, and process logs, which can be employed during the processing of personal data ("Özel Nitelikli Kişisel Verilerin İşlenme Şartları | Kişisel Verileri Koruma Kurulu", n.d.; "2018/10 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurulu", 2018) In line with the implementation of the KVKK, Article 9(4) of the GDPR permits member states to retain or introduce additional conditions, including limitations, related to the processing of genetic data, biometric data, or data concerning health, and certain countries, such as the UK, obliges additional measures for the processing of special categories of personal data. (see "Special Category Data," n.d.)

THE RIGHTS OF DATA SUBJECTS

Data subjects are afforded specific rights under both the GDPR and the KVKK. While certain rights are shared between the two, distinctions and additional entitlements are evident in the GDPR. The subsequent section conducts a comparative analysis of the rights of data subjects, addressing each one individually.

- **Right to Information**

One of the most crucial rights afforded to data subjects is the right to be informed. Accordingly, both the GDPR (Art.12-14) and the KVKK (Art.10) mandate the provision of certain information to data subjects before commencing the processing of their personal data. The right to information is pivotal, as it facilitates the effective exercise of subsequent rights. Therefore, it can be recognized as primus inter pares among other rights (Uršič, 2021, p. 64). Failure to provide necessary information related to processing activities would hinder the ability to maintain control over personal data. Consequently, both legal frameworks necessitate the disclosure of minimum specific information to data subjects. While the GDPR considers the right to information as a right, the KVKK classifies it as an obligation for controllers. Despite this distinction, the ultimate outcome remains the same. Controllers have the flexibility to expand upon this information list, but they are not allowed to limit it. For a detailed comparison of the types of information required for data subjects under the GDPR and KVKK, please refer to Table 3 below.

Table 3:
Information that should be given to applicants under GDPR and KVKK.

Category of Information	**GDPR**	**KVKK**
The identity and contact details of the controller	Art. 13(1)(a)	Art. 10(1)(a)
The contact details of the data protection officer, where applicable	Art. 13(1)(b)	No concept of data protection officer in the KVKK
The purposes of the processing	Art. 13(1)(c)	Art. 10(1)(b)
Legal basis for the processing	Art. 13(1)(c)	Art. 10(1)(ç)
The legitimate interests pursued by the controller or by a third party	Art. 13(1)(d)	X
The recipients or categories of recipients of the personal data and information about the purpose of the transfer	Art. 13(1)(e)	Art. 10(1)(c)
The existence or absence of an adequacy decision	Art. 13(1)(f)	X
Reference to the appropriate or suitable safeguards	Art. 13(1)(f)	X
The period for which the personal data will be stored	Art. 13(2)(a)	X
Existence of rights of data subjects	Art. 13(2)(b), (c), (d)	Art. 10(1)(d)
Provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract	Art. 13(2)(e)	X
The existence of automated decision-making, including profiling and the logic behind it and consequences of it for data subjects	Art. 13(2)(f)	X
The method of collection of personal data	X	Art. 10(1)(ç)
New purposes other than initially expressed	Art.13(3)	X

Regarding the enjoyment of rights, it may seem that the KVKK puts applicants at a disadvantage by not granting them the right to be informed about the existence of automated decision-making, including profiling, the logic behind it, and its consequences. However, the KVKK includes a type of information that the GDPR does not: the method of collection of personal data. If an automated decision-making system will be used at any stage of processing, it should be disclosed to the data subject under the provision of Art.10(1)(ç). Additionally, data subjects may seem to lack the right to be informed about the legitimate interests pursued by the controller or by a third party. However, the Authority accepts the transparency principle in the implementation of the KVKK, so applicants have the right to learn about the legitimate interest pursued in the scope of the right to learn about the processing and purposes. (Art. 11(1)(c) and Art.11(1)(b) of the KVKK).

When implementing the KVKK, the absence of certain types of information, as depicted in the table, can result in the ineffective exercise of data subject rights and complicate processing activities. For instance, the lack of information regarding the retention period poses challenges to the execution of the right to erasure, as data subjects are left uninformed about the duration their personal data will be processed.

Similarly, the omission of details pertaining to adequacy decisions and appropriate safeguards contravenes the transparency principle. This omission makes it challenging for data subjects to evaluate the risks and security implications associated with transmitting their personal data. Without such information, data subjects may hesitate to provide their personal data, even if security measures are in place, and may refrain from giving their explicit consent.

Additionally, the failure to provide information about the necessity of personal data as a statutory or contractual requirement, or as a requirement essential for entering into a contract, hampers transparency. This absence deprives data subjects of the opportunity to assess the conformity of the requested personal data. (Uršič, 2021, p. 67)

Finally, under Article 13(3) of the GDPR, the controller is obligated to inform data subjects about new purposes and relevant information when personal data is collected for purposes other than those initially communicated. While it may appear that the KVKK lacks this condition, the Authority's *"Communique On Principles and Procedures to Be Followed in Fulfillment of the Obligation To Inform"*as stated in Article 5(1)(b), explicitly grants this right to data subjects under the KVKK.

- **Right to Information when personal data is gathered from third parties**

In situations where personal data is acquired from third parties, GDPR Art. 14 mandates the obligation to provide information to data subjects regarding processing activities. Although the KVKK lacks a specific provision regarding the obligation to inform when collecting personal data from third parties, relevant provisions on this matter can be found in the Authority's *"Communique On Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform"* (refer to Authority Communique, 2018). For additional details on the information that should be provided to data subjects in this context, beyond the requirements outlined in Art. 13 of the GDPR and Art. 10 of the KVKK (as shown in Table 3), please consult the table below. Additionally, the table provides information on the timeframe for fulfilling the obligation to inform in such cases.

Table 4:
Different implementations of the information obligation in the GDPR and the KVKK when data collected from third parties

The time of fulfilling the obligation to inform	**GDPR**	**KVKK** (under the provisions of above mentioned Communique)
Within a reasonable period after obtaining the personal data	Art. 14(3)(a)	Art. 6(1)(a) of the Communique
At the latest within one month	Art. 14(3)(a)	X, no obligatory deadline
At the latest at the time of the first communication to that data subject if the personal data are to be used for communication with the data subject	Art. 14/3-b	Art. 6(1)(b) of the Communique
At the latest when the personal data are first disclosed	If a disclosure to another recipient is envisaged, Art. 14(3)(c)	At the time of the first transfer of personal, Art. 6(1)(b) of the Communique
In addition to Art. 13 of the GDPR and Art. 10 of the KVKK, categories of further information should be given to data subjects	**GDPR**	**KVKK** (under the provisions of above mentioned communique)
From which source the personal data originate, and if applicable, whether it came from publicly accessible sources	Art. 14(2)(f)	X
The categories of personal data concerned	Art. 14(1)(d)	X
Existence of the exception available	Exceptions available under Art. 14(5)	No exception available

As depicted in the table, when personal data is obtained from third parties, information about the categories of personal data and the specific sources from which the personal data is collected should be provided to data subjects in the GDPR. This additional information requirement, in practice under the GDPR, is designed to empower data subjects with control over processing activities. In cases where data is collected from third parties, data subjects may be unaware of the specific categories of personal data collected and the sources providing that information (Uršič, 2021, p. 67). Consequently, the absence of this information in the KVKK undermines the sense of control for data subjects.

The timing of the information obligation shows similarities under both laws, as they both aim to provide information to data subjects in a reasonable timeframe. Finally, the GDPR acknowledges certain exceptions to the additional information obligation to strike a balance between the rights of data subjects and controllers.

- **Right of access by the data subjects**

The right of access empowers data subjects to confirm processing activities related to their personal data and acquire information in accordance with the required details. Both legal frameworks grant this right to data subjects through their respective provisions (GDPR Art.15; KVKK Art. 11/(a), Art.11(b)) The right of access is crucial not only for verifying the accuracy of personal data but also for evaluating the lawfulness of processing. Once data subjects access and obtain a copy, they can more effectively exercise their right to object, right to erasure, right to rectification, and right to restriction of processing.

Article 15 of the GDPR and Art. 11/(a), Art.11(b) of the KVKK empowers data subjects to verify whether their personal data is undergoing processing and, if so, to access detailed information about the processing activities. The information obligation linked to the right of access differs from the right to information due to its sequential nature. (Uršič, 2021, p. 104) This distinction implies that the right to information precedes the processing, while the right of information, within the scope of the right of access, comes into play after the processing has occurred. On the other hand, Art.15(3) of the GDPR also allows to request a copy of the personal data undergoing processing. The CJEU, in Case C 579/21 (para 64) and Case C 487/21 (paras 21, 45), interprets the term “copy” as a faithful and intelligible reproduction or transcription of all the data. Therefore, a general description or a reference to categories of personal data does not meet this definition. (Case C 487/21, para 21) The copy provided should encompass all personal data in the processing (Case C 487/21, para 32).

However, providing this copy may pose practical challenges, as it could involve the personal information of others, leading to conflicts between the rights of data subjects and the rights of third parties. Therefore, controllers may erroneously view protecting the rights of others as a restriction on data subjects' rights of access under Article 23 of the GDPR, avoiding their obligation to provide a copy. Nevertheless, in such situations, controllers must strike a balance, as emphasized by the CJEU in Case C 579/21 (para 80). It is not acceptable to infringe upon the rights of others or to use their rights as a pretext for neglecting data subjects’ rights (Case C 579/21, para 80) In these circumstances, controllers should prioritize utilizing available means to fulfill their obligations without violating anyone's rights (Case C 579/21, para 80).

In the context of the KVKK, the legislation doesn't explicitly use the term "the right of access." Instead, it employs the phrase "data subjects may request whether their personal data is processing and, if so, information about personal data processing activities." There is room for debate on whether this encompasses the obligation to provide a copy concerning processing activities. However, it's crucial to note that the Turkish Constitution explicitly affirms, in Article 20, the right of every individual to access their personal data. Therefore, the absence of the specific mention of the right to request a copy should not be misconstrued to imply that data subjects cannot request a copy from controllers, given that "access" is constitutionally guaranteed. Ideally, it would be beneficial if the KVKK directly incorporated the right of access to a copy into its provisions. However, the interpretation by the CJEU regarding the "copy" of processing activities should be considered applicable to the KVKK as well, as it represents a form of utilizing the right to access.

- **Right to rectification**

GDPR Art. 16 and KVKK Art.11(1)(d) confer upon data subjects the right to rectification, allowing them to request the correction or modification of their personal data. Processed personal data often

carries consequences, be they positive or negative, for individuals. For instance, banks determine credit scores, employers conduct performance evaluations, commercials engage in advertising and marketing, and legal decisions are made by public authorities, all based on the processing of personal data. Consequently, the accuracy of the personal data undergoing processing is essential for data subjects. Therefore, both laws, by ensuring the right to rectification, safeguard the rights and interests of data subjects under their respective provisions.

- **Right to erasure**

In the current landscape, the right to erasure stands out as a pivotal post hoc empowerment measure within the data protection framework. (Ausloos, 2020, p.105) Because permanently recording rises vulnerabilities for individuals by leading to recurrent data breaches and potential unforeseen or undesirable future uses. (Ausloos, p.106) The right to erasure is conferred upon data subjects by GDPR Art. 17 and KVKK Art.11(1)(e). According to GDPR Art.17, data subjects have the right to request the erasure of their personal data. However, controllers may not be obligated to comply with such requests immediately. As outlined in Article 17 of the GDPR, controllers can persist in processing personal data if it remains necessary for the original purpose of collection. Even if a data subject withdraws their consent, controllers may still process personal data if another legal basis is available, or they may continue processing based on legitimate interests if an overriding interest exists. However, in cases where processing is deemed unlawful, controllers are obligated to erase the personal data of data subjects. Exceptions to the right to erasure are regulated under 17(3)(e) and 17(3)(b) for situations where controllers have a legitimate interest in establishing, exercising, or defending a legal claim or a legal obligation for processing.

Regarding the KVKK, the right to erasure is not as detailed as in the GDPR. Art.11(e) of the KVKK states that in the event the reasons for processing cease to exist, a data subject may request the erasure of their personal data. However, this is applicable only if the processing was initially lawful. If the processing is unlawful, data subjects can still demand erasure under the KVKK. As discussed under the title of consent, even though there is no separate provision for it, if data subjects withdraw their consent, they can request erasure of their personal data since processing becomes unlawful after withdrawal. Concerning legitimate interest, the approach of the GDPR would similarly apply to the KVKK, even in the absence of a specific provision. If a controller lacks an overriding and balanced interest, processing based on legitimate interest would be deemed unlawful, necessitating erasure either ex officio or upon the demand of data subjects.

- **Right to restriction of processing**

While the GDPR affords data subjects the right to restrict processing, the KVKK lacks a similar provision. The right to restrict processing is paramount in bolstering control over the personal data of data subjects. It enables the temporary suspension or limitation of processing, validating objections from data subjects regarding processing accuracy or in cases where such processing conflicts with the legitimate interests of controllers. Furthermore, this right empowers data subjects to object to erasure, even if the processing is deemed unlawful or the personal data is no longer required for its original purpose, but is still necessary for the establishment, exercise, or defense of legal claims by data subjects.

- **Right to request notification**

GDPR Article 19 and KVKK Article 11(1)(d) delineate the right to notification, empowering data subjects to compel controllers to inform all recipients of their personal data about any imposed restrictions, erasures, or rectifications. By exercising this right, data subjects actively verify and ensure the accuracy of their personal data. While the GDPR includes a balancing provision, affirming that the notification obligation stands unless it necessitates disproportionate efforts, the KVKK lacks a corresponding exception, making this duty obligatory for controllers subject to the KVKK. Relying on the disproportionate effort exception is tough since it involves a careful assessment to weigh the importance of not informing recipients against the burden of the effort needed. ("Are There Any Exceptions?," n.d.) However, in certain situations, this exception is crucial. For instance, if not informing recipients wouldn't harm data subjects, but the effort required for notification is just too much. Therefore, in situations where controllers subject to the KVKK receive notification requests that entail disproportionate efforts, they may have to depend on general legal principles, such as the abuse of a right or the violation of good faith.

- **Right to data portability**

One of the rights regulated by the GDPR through Article 20 but absent in the KVKK is the right to data portability. This right in the GDPR allows a data subject to obtain and/or transmit a copy of personal data concerning him/her in a structured, commonly used, and machine-readable format if the processing is based on consent or the performance of a contract and is carried out by automated means. This right is also applicable for personal data which is provided by data subjects. Therefore, because the restrictions about the way of obtaining data, the way of processing data and legal ground of processing it is fair to say that application of this right comparatively limited.

It is accurate to assert that the right to data portability and the right to data access within the scope of the GDPR share similarities. However, the right to data portability extends beyond mere access, enabling individuals not only to access their data but also to transmit it to other controllers in a more suitable manner and in a machine-readable format. (Uršič, 2021, p.171) Consequently, the right to data portability can be viewed as an advanced version of the right to access.

From the perspective of personal data protection, the right to data portability enhances individuals' control over their personal data. A data subject can exercise this right if dissatisfied with their service provider, allowing them to switch to another provider while safeguarding the processing of their personal data, thereby avoiding the loss of essential data (Uršič, 2021, p.181). Moreover, this right promotes transparency in data processing, enabling data subjects to manage their online identities and facilitate secure data flows (Uršič, 2021, p.187). Despite being relatively new in the context of the GDPR, the scope and exercise of this right contribute to data subjects in various ways, such as increasing competition among controllers in favor of data subjects (Uršič, 2021, pp.174-178) and enhancing consumer protection by encouraging service providers to create a more consumer-friendly online environment (Uršič, 2021, pp.178-180) Consequently, if the KVKK had included this right in its scope, it would have brought greater control and benefits to data subjects.

- **Right to object**

The absence of the right to object in the KVKK stands in contrast to the GDPR, which, through Article 21, grants data subjects the power to object to the processing of their personal data, including profiling based on the legitimate interests of controllers or public interest. When a data subject exercises the right

to object, the controller must cease processing personal data unless it can demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the individual or are necessary for the establishment, exercise, or defense of legal claims. (Art.21(1) of the GDPR)

The right to object serves as the initial step toward the right to be forgotten (Uršič, 2021, p.201) as it opens the door to challenging the legitimacy of processing. Furthermore, the right to object strengthens the lawfulness of processing personal data relying on legitimate interest by compelling controllers to conduct careful balancing tests to avoid objections to this processing. Thus, it upholds fairness principles (Uršič, 2021, p.202) by aligning the expectations of the data subject regarding that specific processing and the intention of the controller.

The absence of this right under the KVKK puts data subjects in a disadvantageous position as there is potential harm to the data subject if a balancing test is not conducted efficiently and fairly. On the other hand, it is a fact that many businesses conduct profiling activities in their operations, which have effects on individuals. An objection mechanism empowers data subjects by giving them control over the use of their personal data, especially when negative outcomes result, such as an increase in insurance payments or job dismissal (Uršič, 2021, p.202)

Finally, Article 21(2) of the GDPR grants an absolute right to object to direct marketing. This is because both direct marketing and the collection of personal data for direct marketing purposes constitute a severe interference with the data subject's privacy (Uršič, 2021, p.204). Thus, regardless of the legal grounds, data subjects have the unequivocal right to object to direct marketing, and controllers must cease processing without any opportunity to compel the objection. This right is evidently designed to shield data subjects from online profiling activities and enhance privacy. Consequently, it would be advantageous for the KVKK to incorporate a similar right. Although data subjects already possess the right to object to direct marketing through other legislations like e-commerce and/or e-communication, from the perspective of personal data protection, providing the right to object to processing for direct marketing aligns with the principles of safeguarding privacy.

- **The right not to be subject to solely automated decisions**

While Article 22 of the GDPR governs the right not to be subjected to solely automated decisions, KVKK Article 11(1)(g) similarly states that data subjects have the right to object to the results of decisions based solely on automated processing, albeit with partial alignment. The scope of these two rights, however, differs. Under GDPR implementation, data subjects may request not to be subjected to solely automated decision-making with legal effects on them. However, this right is not absolute, as Article 22(2) provides exceptions. These exceptions pertain to the basis of the decision, specifically: if the solely automated decision is necessary for entering into or performing a contract between the data subject and a data controller, or if it is based on the data subject's explicit consent, or if it is authorized by Union or Member State law to which the controller is subject. As evident, the scope of this right is narrowed not only by exceptions but also inherently as it is debatable if a decision is solely based on automated processes when human interference is involved in the decision-making process. (Uršič, 2021, p.206) Yet, when decisions rely solely on automated processes, this right serves data subjects by shielding them from outcomes that arise through the categorization, assessment, and discrimination carried out by automated activities—an occurrence that has become more prevalent with the advancement of technology. In the implementation of the KVKK, the scope of this right differs, as the objection is not directed towards being subject to solely automated decision-making processes but rather towards the results produced by them. As a concise summary of this chapter, please refer to the concluding table.

Table 5:
Rights under the GDPR and KVKK and linked principles&legal grounds

Data Subject Rights under the GDPR	Related Principles	Related Legal Grounds
Right to be informed; GDPR Art.12-14, KVKK Art.10	Fairness, Transparency	For all legal bases
Right of access by the data subjects; GDPR Art. 15, KVKK Art. 11/(a), Art.11(b)	Fairness, Transparency, Accountability	For all legal bases
Right to rectification; GDPR Art. 16, KVKK Art.11(1)(d)	Accuracy	For all legal bases
Right to erasure; GDPR Art. 17, KVKK Art.11(1)(e) (partially similar, just saying data subjects are given the right to erasure, no detailed explanations like in the GDPR	Storage limitation, Purpose limitation, Lawfulness	For all legal bases but consent and legitimate interest have their own conditions
Right to restriction of processing; GDPR Art. 18, KVKK Missing	Accuracy, Lawfulness, Purpose limitation	For all bases
Right to request notification; GDPR Art. 19, KVKK Art.11(1)(d)	Accuracy	For all bases
Right to data portability; GDPR Art.20, KVKK Missing	Integrity, Confidentiality	Consent, Performance of a contract, not applicable for public interest
Right to object; GDPR Art. 21, KVKK Missing	Fairness, Purpose limitation	Public interest, Legitimate interest
Right to object for direct marketing; GDPR Art.21(2), KVKK Missing	Fairness	For all bases
Right to object automated individual decision-making; GDPR Art. 22, KVKK Art.11(1)(g) (partially similar, it is stated that data subjects have the right to object to the results of decisions based solely on automated processing)	Fairness	For all bases

CONCLUSION

In comparing the GDPR and KVKK, we observe a high level of compatibility in terms of the fundamental principles governing data processing. While some principles may appear absent in the KVKK, a holistic interpretation of its provisions and the Authority's guidance reveals an implicit recognition of these principles. Furthermore, the principles explicitly stated in the KVKK align precisely with those in the GDPR. Despite the KVKK not explicitly elaborating on these principles by default, the Authority fills this gap, ensuring a comprehensive understanding.

However, differences emerge between the two laws, particularly regarding the legal grounds for data processing. Unlike the GDPR, the KVKK lacks concrete results based on legal grounds and does not aim to grant data subjects specific rights based on legal grounds. Notably, the legal basis of legitimate interest, the right to object to processing based on this, and the clarity of the balancing test are inadequately addressed, leaving a gap that could disadvantage data subjects. The absence of the concept of processing in the public interest in the KVKK complicates discussions about whether processing

genuinely serves the public interest, creating challenges for private-sector processors undertaking public duties. Furthermore, while the KVKK lacks separate provisions for consent, the Authority has bridged this gap.

While the GDPR presents exceptions to the prohibition of processing special categories of data, including consent, the KVKK strictly prohibits processing without consent and provides specific processing bases for certain special category data types. Although the GDPR might seem initially more limited due to its acceptance of exceptional processing, the exceptions it offers are more comprehensive and appropriate, while the KVKK's determined legal bases for special categories of data remain restrictive.

Lastly, when considering the rights of data subjects, it becomes evident that the KVKK offers fewer rights and lacks detailed implementation in comparison to the GDPR. Specifically, the absence of the right to object, the right to restriction of processing, and the right to data portability diminish the sense of control that data subjects have over their personal data. Furthermore, due to the unclear nature of the KVKK, the right to copy within the scope of the right to access is not clearly defined, putting data subjects at a disadvantage.

In conclusion, while the KVKK demonstrates basic compatibility with the GDPR, this alignment stems more from the proactive efforts of the Authority than the inherent features of the KVKK itself. The KVKK falls short of the GDPR in balancing the rights and interests of parties, and its lack of detailed provisions occasionally places data owners and processors at a disadvantage. However, because its compatible basic construction allows this, a holistic approach and meticulous study could easily render the KVKK fully compatible with GDPR.

REFERENCES

Açık Rıza | Kişisel Verileri Koruma Kurumu. (n.d.). Retrieved from https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf

Açık Rıza Alırken Dikkat Edilecek Hususlar | Kişisel Verileri Koruma Kurumu. (n.d.). Retrieved from https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar

Alenileştirme" Hakkında Kamuoyu Duyurusu | Kişisel Verileri Koruma Kurumu. (2020). Retrieved from https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU

Are there any exceptions? (n.d.). Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/are-there-any-exceptions/#id4

Ausloos, J. (2020, January 1). *The Right to Erasure in EU Data Protection Law*. http://books.google.ie/books?id=eYyjzQEACAAJ&dq=The+Right+to+Erasure++in+EU+Data++Protection+Law&hl=&cd=1&source=gbs_api

Besemer, L. (2020). *PRIVACY AND DATA PROTECTION*. Retrieved from http://books.google.ie/books?id=ZMTXzQEACAAJ&dq=Privacy+and+Data+Protection+based+on+the+GDPR&hl=&cd=2&source=gbs_api

Bilir F. (2020). The Review of 6698 Numbered Personal Data Protection Law and Protection of Personal Data in the Internet Age. Anayasa Yargısı, Cilt: 37, Sayı: 2, s.305–342. Retrieved from https://ayam.anayasa.gov.tr/media/6686/04_faruk_bilir.pdf

Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) | European Data Protection Board. (n.d.). Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en

Case C 487/21 (2023) Österreichische Datenschutzbehörde, v. CRIF GmbH

Case C-579/21 (2023) *J.M. v. Apulaistietosuojavaltuutettu, Pankki S*

Communique on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform | Kişisel Verileri Koruma Kurumu. (2018). Retrieved from https://www.kvkk.gov.tr/Icerik/6637/Communique-On-Principles-And-Procedures-To-Be-Followed-In-Fullfillment-Of-The-Obligation-To-Inform

Develioğlu M.(2017). 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul: On İki Levha Yayıncılık.

Dienst S.(2017). Lawful processing of personal data in companies under the GDPR. D. Rücker &T. Kugler (Eds.). *New European General Data Protection Regulation: A Practitioner's Guide* (pp.49-103)

Doğru Bilinen Yanlışlar 2 | Kişisel Verileri Koruma Kurumu. (n.d.) Retrieved from https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2

Europe, C. O., & Rights, E. U. A. F. F. (2018). *Handbook on European data protection law*. Council of Europe. Retrieved from http://books.google.ie/books?id=X_OFDwAAQBAJ&pg=PP2&dq=978-92-871-9849-5&hl=&cd=1&source=gbs_api

Guidelines on Data Protection Officers ('DPOs') | Article29 Working Party. (2017). Retrieved from https://ec.europa.eu/newsroom/article29/items/612048

Han, I. A., Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 18(1), 417-459

Kaya, M. B. (2021). The New Paradigm of Data Protection Law: The Principle of Accountability. *İstanbul Hukuk Mecmuası*. https://doi.org/10.26650/mecmua.2020.78.4.0005

Kişisel Veri İşleme Şartları | Kişisel Verileri Koruma Kurumu. (n.d.). Retrieved from https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari

Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu | Kişisel Verileri Koruma Kurumu. (2019). Retrieved from https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu

Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" | Article 29 Data Protection Working Party (n.d.), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Özel Nitelikli Kişisel Verilerin İşlenme Şartları | Kişisel Verileri Koruma Kurulu.(n.d.). Retrieved from https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari

Press Release No 158/22 |Court of Justice of the European Union", 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158en.pdf

Rücker, D., & Kugler, T. (2017). *New European General Data Protection Regulation*. Nomos/Hart. Retrieved from http://books.google.ie/books?id=Ru7pswEACAAJ&dq=Tobias+Kugler&hl=&cd=1&source=gbs_api

Sıkça Sorulan Sorular | Kişisel Verileri Koruma Kurumu. (2019). Retrieved from https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular

Special category data. (n.d.). Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

Temel İlkeler | Kişisel Verileri Koruma Kurumu. (n.d.). Retrieved from https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler

The Criteria for The Determination of Countries Having an Adequate Level of Protection | Kişisel Verileri Koruma Kurulu. (2019). Retrieved from https://www.kvkk.gov.tr/Icerik/6642/Transfer-of-Personal-Data-Abroad

The Eleventh Development Plan | Presidency of Republic of Turkey Presidency of Strategy and Budget. (2019). Retrieved from https://www.sbb.gov.tr/wp-content/uploads/2022/07/Eleventh_Development_Plan_2019-2023.pdf

Uçak, M. (2021). Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası. Kişisel Verileri Koruma Dergisi, 3(1), 41-60.

Uršič, H. (2021). *Data Subject Rights Under the GDPR*. Retrieved from http://books.google.ie/books?id=SECizgEACAAJ&dq=HELENA+U.+VRABEC&hl=&cd=1&source=gbs_api

Ustaran, E. (2022). *European Data Protection, Third Edition*. Retrieved from http://books.google.ie/books?id=6AFGzwEACAAJ&dq=978-1-948771-72-6&hl=&cd=1&source=gbs_api

Van Alsenoy, B. (2019). *Data Protection Law in the EU*. Retrieved from http://books.google.ie/books?id=xfwiwwEACAAJ&dq=9781780688459&hl=&cd=3&source=gbs_api

Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler| Kişisel Verileri Koruma Kurulu. (n.d.). Retrieved from https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler

2018/10 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurulu. (2018). Retrieved from https://www.kvkk.gov.tr/Icerik/4110/2018-10

2019/125 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurulu. (2019). Retrieved from https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari

2020/173 sayılı Kurul Kararı | Kişisel Verileri Koruma Kurumu. (2020). Retrieved from https://www.kvkk.gov.tr/Icerik/6739/2020-173