JPEPFM Journal of Public Economy and Public Financial Management

Kamu Ekonomisi ve Kamu Mali Yönetimi Dergisi, Cilt: 5 | Sayı: 1 | Nisan 2025

Journal of Public Economy and Public Financial Management, Volume: 5 | Issue: 1 | April 2025

BALANCING EXCEPTIONS AND PRINCIPLES IN KVKK: A CRITICAL ANALYSIS

Cihan ÜNAL[1]

Hakan YILDIRIM[2]

Ayhan BÜTÜNER[3]

Recieved (First): *07.02.2025* ***Accepted:*** *17.03.2025*

Citation/©: Ünal, C., Yıldırım, H. & Bütüner, A. (2025). Balancing Exceptions and Principles in KVKK: A Critical Analysis, *Journal of Public Economy and Public Financial Management, 5*(1), 1-27.

Abstract

The purpose of the Law on the Protection of Personal Data No. 6698 (KVKK) is to protect individuals' fundamental rights and freedoms during the processing of personal data and to define the obligations of data controllers. The fundamental principles outlined by the law, ensuring the lawful processing of personal data, play a critical role in data processing activities. However, Article 28 of the law introduces certain exceptions, particularly concerning public and economic security, providing exemptions in specific cases. In practice, ensuring that these exceptions align with the general principles of the law is considered a legal necessity.

This article examines how the exceptions outlined in Article 28 of KVKK should be balanced with the law's general principles. The practical challenges of applying these exceptions, especially in data processing activities related to public and economic security, are evaluated through concrete examples involving institutions such as the General Directorate of Security (EGM) and the Financial Crimes Investigation Board (MASAK). Additionally, a comparative analysis is conducted with the General Data Protection Regulation (GDPR) of the European Union and U.S. laws such as the California Consumer Privacy Act (CCPA), highlighting KVKK's alignment with international data protection standards. Despite aligning with global standards, Turkey's KVKK struggles with practical challenges in applying exception provisions, especially in balancing privacy with public security

Lastly, recommendations are provided for strengthening oversight mechanisms, increasing transparency in data processing, and ensuring better protection of personal data.

Keywords: KVKK, General Principles, Exception, Public Security, International Comparison.

JEL Codes: *K20, H10, and O38.*

1. INTRODUCTION

In the digital age, personal data is as valuable as currency. But how do we balance individual privacy with the needs of national security? With the rapid development of the digital age, the protection of personal data has become a critical issue worldwide. As the secure processing and storage of personal data become increasingly important for safeguarding individuals' privacy, states and institutions feel the need to establish comprehensive regulations in this area (Çubukçu, 2024). In Turkey, the Personal Data Protection Law No. 6698 (KVKK) was enacted to address this need and to protect individuals' fundamental rights and freedoms. KVKK establishes general principles, such as compliance with the law, fairness, data minimization, and purpose limitation, which must be adhered to during the processing of personal data, and imposes significant obligations on data controllers (Oğuz, 2018).

[1]Dr, Hacettepe University, cihan.unal@hacettepe.edu.tr, Orcid no : 0000-0002-5255-4078, (Correspondig)
[2]Dr, Ankara Bilim University, hakanyildirim72@gmail.com , Orcid no : 0000-0002-5959-2691
[3]Konya National Education, butunerayhan@gmail.com, Orcid no : 0009-0003-8589-7792

This article examines the alignment of Turkey's Personal Data Protection Law No. 6698 (KVKK) with international data protection standards, focusing on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and the General Data Protection Regulation (GDPR) of the European Union (Council of Europe, 1981).

Convention 108, adopted by the Council of Europe in 1981, serves as the first binding international instrument to protect individuals against abuses which may accompany the collection and processing of personal data. While it establishes basic principles for data protection and the rights of individuals, its provisions are less detailed compared to the GDPR, which was adopted by the European Union in 2016 and came into effect in 2018. The GDPR provides a more comprehensive and detailed framework for data processing rules and expands the rights of individuals significantly. (Bertoni, 2021)

Both frameworks lay down fundamental principles for the processing of personal data. However, GDPR elaborates on these principles in greater detail and with stricter enforcement, emphasizing data minimization, accuracy, storage limitation, and integrity. It also defines the obligations of data controllers and processors with enhanced accountability to comply with these principles.

The GDPR grants individuals expanded rights such as the right to erasure, data portability, processing restrictions, and the right to object, making it more comprehensive compared to Convention 108. While Convention 108 allows flexibility for member states to adapt its principles into national laws, the GDPR is directly applicable and uniformly enforced across all EU member states (Council of Europe, 1981).

This analysis will examine how KVKK aligns with these international standards, identifying its similarities and differences with GDPR and Convention 108. Considering that Article 9 grants countries the authority to establish exceptions, the discussion will also explore the implications of these divergences for personal data protection in Turkey and potential areas for improvement to meet global data protection standards.

In addition to the general principles of KVKK, the exception provisions outlined in Article 28 also stand out. These provisions define certain limitations and exemptions regarding the protection of personal data, particularly in areas such as national security, public safety, and economic security. However, the scope of these exceptions has led to various debates in practice. One of the fundamental principles of law is that the obligation to comply with the general principles of the law must continue even within the scope of these exceptions (Işık, 2022). On the other hand, in practice, it has been observed that the principles of data minimization, transparency, and proportionality are sometimes violated in data processing activities carried out for reasons of public security. This situation has caused serious challenges in balancing the protection of personal data with the public interest (Aydın, 2024).

The protection of personal data holds great importance in today’s digital age. The Personal Data Protection Law No. 6698 (KVKK) is the most significant legislation defining the legal framework in this area in Turkey. KVKK regulates the general principles that must be followed in data processing activities and the sanctions to be applied in cases of violation. (Yücedağ, 2019)

KVKK aims to protect individuals' fundamental rights and freedoms during the processing of personal data and to define the obligations of data controllers. This law sets out the necessary rules for the lawful processing, storage, and sharing of personal data.

Article 4 of KVKK, which follows the sections on purpose, scope, and definitions, lists the general principles to be followed in the processing of personal data. These principles include conducting data processing activities in a lawful, fair, and transparent manner, ensuring the accuracy and currency of the data, processing data for specific, explicit, and legitimate purposes, ensuring that the processing is relevant, limited, and proportionate to its purpose, and retaining the data only for the duration required by the relevant legislation or the purpose for which it was processed.[4] (Kişisel Verileri Koruma Kurumu, 2024) When the purpose of processing is "intelligence gathering," and other rules and regulations are not considered alongside it, this automatically results in a complete disregard for any boundaries (Yücedağ, 2019).

Article 28 of KVKK outlines the exceptions where the law will not apply in certain situations. These exceptions include the processing of data for scientific, historical, literary, or artistic purposes, as well as for national defense, national security, public safety, public order, or economic security. In many documented cases, it is understood that these exception provisions have been utilized, particularly in matters concerning public and economic security (Atlı, 2019).

At this point, a problem arises: being exempt from the law does not mean being exempt from the fundamental principles of the law. Institutions and organizations that benefit from the exception provisions are still obligated to comply with other laws and the principles of this law. Furthermore, it cannot be assumed that articles containing exceptions are not subject to the fundamental principles of law. It is also clear that institutions and organizations benefiting from exception provisions are bound by general and specific regulations they are required to follow[5] (Gözler, 2012).

From an international perspective, Turkey's KVKK regulation aligns with the European Union's General Data Protection Regulation (GDPR) and state-level regulations in the United States. Although there is no federal law equivalent to the GDPR in the U.S., laws such as California's California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) provide extensive rights to data subjects. These laws impose significant obligations on businesses in data processing activities and mandate strict measures to ensure data security. Similarly, Virginia's Virginia Consumer Data Protection Act (VCDPA) and Colorado's Colorado Privacy Act (CPA) aim to protect individuals' privacy at the state level by offering data protection provisions similar to the GDPR. In this context, it is evident that KVKK is based on universal data protection principles and has gained an international character (Kaya & Tolun, 2020).

In this article, various concrete cases regarding the application of exception provisions and the documents reflected from these cases have been examined. In this context, how compliance with general principles can be ensured has been discussed. It has been illustrated with examples from

[4] Kişisel Verileri Koruma Kurumu. KVKK Madde 4 - Genel İlkeler. Retrieved June 20, 2024, from https://www.kvkkarar.com/kvkk-madde-04/

[5] Gözler, K. (2012, Eylül 29). Hukuk Yorum İlkeleri. Paper presented at the 'Interpretation and Norm Concretization in Constitutional Law' meeting organized by the Platform of Public Law Scholars and the Union of Turkish Bar Associations, Ankara. https://www.anayasa.gen.tr/yorum-ilkeleri.pdf

the literature, the interpretations of responsible institutions, and concrete cases that exceptions should indeed remain exceptional, and that even within this scope, adherence to the principles of this law is mandatory when processing personal data.

It is evaluated through case studies that the general principles are valid under all circumstances and must be adhered to, and that exception provisions may limit the effectiveness of the law due to challenges in implementation.

Particularly in matters related to public safety and economic security, the practices of institutions such as the General Directorate of Security (EGM) and the Financial Crimes Investigation Board (MASAK), based on exception provisions, have been documented in official records. These practices have been evaluated to determine whether they align with the general principles of the law. (Case Studies, 2022-2024)

These institutions define their activities as intelligence data collection. However, the reliability of intelligence data, the requirement for it to be obtained through legal means, and the necessity of supporting it with other/external sources must be taken into consideration (Özkaya & Toprak, 2022).

At this point, it can be observed that some institutions, relying on the exception provisions of the law, do not adequately consider their obligation to comply with other regulations and general principles.

Challenges related to data security have led to issues that may deviate from the general purpose of the law and have been evaluated within the framework of general surveillance practices. For instance, the primary objective of MASAK (the Financial Crimes Investigation Board) is to combat money laundering. However, it has been observed that MASAK now has online access to all banking transactions of all banks, covering all amounts and time periods. Problems have been noted in ensuring data security and integrity, keeping data up-to-date, and obtaining data through lawful means (Case Studies, 2022-2024).

A similar situation applies to the General Directorate of Security (EGM). Analyzing official documents and correspondence reflected in court cases reveals that all available data regarding an individual, whether private or legal entities, has been collected. It has been determined that these data were not obtained lawfully, no consideration was given to timeframes, no distinction was made between significant and insignificant information, special laws were disregarded, other legal provisions were violated, and principles such as proportionality, data minimization, and purpose limitation were breached. Most importantly, it was found that the data had been tampered with or even manipulated.

Processing, evaluating, and effectively using such extensive datasets is thought to pose various challenges in practice. As a result, a law created to regulate the use of personal data and its fundamental principles is being violated through the exploitation of exception provisions, effectively rendering the law and its principles ineffective and invalid.

The Constitution and laws primarily protect the individual, particularly against the state. However, when it comes to the constitutional provision of protecting individuals' personal data and privacy, these protections have become ineffective. In well-known murder cases, mafia

relations, or similar incidents reflected in the media, it has been observed that there is no oversight or supervision regarding the use of these data. For instance, phone records, HTS (Historical Traffic Search) data, expenditures, and virtually anything reflected in the digital environment are being accessed instantly by institutions such as the General Directorate of Security (EGM) and MASAK under the exception provisions of this law. These data are used with unlimited authority, without oversight, and in a manner that cannot ensure their accuracy or reliability. These occurrences have been directly documented in the official correspondence of these institutions (Case Studies 2022-2024).

It is evident that there is no need for a new regulation on this matter, as KVKK closely resembles its counterpart, GDPR, in Europe and similar regulations in the United States. The main issue here appears to be a misinterpretation of the law, a failure to attach the necessary importance to the concept of "personal data," or, at times, an insufficient understanding of it. It can also be said that the use of keywords such as "exception" and "intelligence" has led to a preconceived notion that unlawful actions and practices can suddenly become lawful. The state's activities in this regard must also comply with the law, adhere to fundamental principles of law, abide by the regulations governing its operations, and conform to the general principles of KVKK. This obligation must be maintained even in the context of "exception" and "intelligence"[6] [7] (Cimer1, Cimer2, 2024).

In this article, using examples and statements from official documents issued by EGM and MASAK, it has been demonstrated that being exempt from the law is perceived as an exemption from general principles and other laws as well, and that the concept of personal data is not fully understood. These findings are illustrated through examples and the table prepared based on them (Table 3 summarizes these results).

This article has been prepared in accordance with academic writing and research ethics guidelines. The sources reported as case studies were used with the consent of the data subjects. All sources used throughout the study have been properly cited to avoid plagiarism, and the principles of honesty, transparency, and impartiality have been adhered to during the research process. Legal regulations, personal data protection laws, and ethical values have been observed. Furthermore, no human or animal subjects were used during the research, and ethical committee approval was not required.

This article examines the necessity of balancing and applying the exceptions listed in Article 28 of KVKK with the general principles of the law and evaluates the challenges encountered in practice using concrete examples. The requirement for data processing activities to align with the general principles of the law in sensitive areas such as national security and public safety will be discussed, focusing on the data processing practices of institutions like the General Directorate of Security (EGM) and the Financial Crimes Investigation Board (MASAK). Additionally, comparisons with GDPR and similar regulations in the United States are made to discuss how KVKK aligns with international data protection standards.

[6] CİMER1. (April 22, 2024). Application and response dated 22.04.2024 with reference number 2401432268 through CİMER.

[7] CİMER2. (May 9, 2024). Application and response dated 09.05.2024 with reference number 2401629279 through CİMER.

2. PROCESSING OF PERSONAL DATA

2.1. Methodology

This study employs a qualitative research approach to evaluate the compatibility of the exception provisions in Turkey's Personal Data Protection Law (KVKK) with the general principles of data protection. The methodology consists of the following components:

Document Analysis: Official documents, reports, and correspondences from institutions such as the General Directorate of Security (EGM) and the Financial Crimes Investigation Board (MASAK) were reviewed. These documents were analyzed to identify potential violations of general principles in data collection and processing activities.

Comparative Legal Analysis: A comparison was conducted between the exception provisions in KVKK and international data protection regulations, including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This comparative approach highlights KVKK's alignment with global data protection standards and identifies areas where the law may diverge or require improvement.

Case Study Analysis: Selected real-life examples and case studies were used to evaluate the practical application of exception provisions. These cases, drawn from administrative court records, demonstrate how public institutions handle personal data within the scope of Article 28 of KVKK and whether they adhere to the principles of transparency, proportionality, and purpose limitation.

Ethical Considerations: The study adheres to research ethics by ensuring the confidentiality and consent of data subjects when analyzing case studies and official documents. No human or animal subjects were directly involved in the research process, and all sources were properly cited to maintain transparency and academic integrity.

2.2. General Principles of KVKK

The Personal Data Protection Law No. 6698 (KVKK) establishes the fundamental principles to be followed during the processing of personal data. These principles ensure that data processing activities are carried out in compliance with legal and ethical standards. The general principles of KVKK are as follows;

Compliance with the Law and Rules of Integrity: The processing of personal data must comply with all relevant legal regulations and the rules of integrity. This means that data processing activities should be carried out transparently, fairly, and within the framework of the law.

Accuracy and Being Up-to-Date When Necessary: Processed personal data must be accurate and kept up-to-date when necessary. The accuracy and currency of data are critical for protecting individuals' rights and ensuring the effectiveness of data processing activities.

Processing for Specific, Explicit, and Legitimate Purposes: Personal data must be processed for specific, explicit, and legitimate purposes. The purpose of data processing activities should be clearly defined, and processing should not extend beyond these purposes.

Being Relevant, Limited and Proportionate to the Purpose for Which They Are Processed

Personal data must be relevant, limited, and proportionate to the purposes for which they are processed. This means that only necessary data should be processed, and data processing activities should remain strictly within the scope of their intended purpose. In this context, even if all legal requirements are met, the principle of data minimization must never be violated while using data in line with adequacy and purpose. (Yosif, 2021)

Retention for the Period Prescribed by Relevant Legislation or Required for Processing Purposes: Personal data must be retained only for the period prescribed by relevant legislation or as necessary for the purposes for which they are processed. Unnecessary data retention periods should be avoided to ensure data security and privacy.

These principles form the foundation of KVKK and ensure that personal data processing activities are carried out in compliance with legal and ethical standards. Even the exceptions specified in Article 28 of the law must align with these general principles. Data processing activities, even in exceptional cases, should be conducted in accordance with these fundamental principles. The general principles are almost identical, with minor differences, to those found in similar regulations in Turkey and around the world.

2.3. Comparison of KVKK General Principles and GDPR General Principles

Below, in Table 1, the general principles of Turkey's Personal Data Protection Law (KVKK) are compared with those of the European Union's General Data Protection Regulation (GDPR).

Table 1. Comparison of KVKK General Principles with GDPR

General Principle	General Principle	GDPR (EU)
Compliance with Law and Integrity	Personal data must be processed lawfully and in accordance with the rules of integrity	Personal data must be processed lawfully, fairly, and transparently
Accuracy and Being Up-to-Date	Personal data must be accurate and kept up-to-date when necessary.	Personal data must be accurate and kept up-to-date.
Processing for Specific, Explicit, and Legitimate Purposes	Personal data must be processed for specific, explicit, and legitimate purposes.	Personal data must be collected and processed for specified, explicit, and legitimate purposes.
Relevance, Limited Scope, and Proportionality	Personal data must be relevant, limited, and proportionate to the purposes for which they are processed.	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes.
Retention Limitation	Personal data must only be retained for the period prescribed by law or as required for processing purposes.	Personal data must not be kept longer than necessary for the purposes for which it is processed.

General Principle	General Principle	GDPR (EU)
Compliance with Law and Integrity	Personal data must be processed lawfully and in accordance with the rules of integrity	Personal data must be processed lawfully, fairly, and transparently
Security and Confidentiality	Personal data must be protected against unauthorized or unlawful processing, loss, destruction, or damage through appropriate security measures.	Personal data must be protected against unauthorized or unlawful processing, loss, destruction, or damage through appropriate technical and organizational measures.
Accountability	Data controllers may face administrative or legal penalties, but oversight mechanisms are weak or absent.	Data controllers are required to demonstrate compliance with GDPR, supported by rigorous oversight and accountability mechanisms.

Source: Prepared by the authors based on their analysis.

As shown in Table 1, both KVKK and GDPR prioritize fundamental principles such as lawfulness, fairness, purpose limitation, and data security. These shared values ensure that personal data is processed ethically and responsibly under both frameworks.

Accountability Mechanisms: GDPR introduces stricter accountability requirements (e.g., Data Protection Impact Assessments and mandatory appointment of Data Protection Officers), as highlighted in the Accountability row of Table 1. In contrast, KVKK has weaker enforcement mechanisms and lacks robust oversight systems to ensure compliance.

Oversight and Enforcement: GDPR's detailed mechanisms for demonstrating compliance create greater transparency, whereas KVKK relies more on administrative or legal penalties, as noted under Accountability in Table 1.

Enhancing Accountability in KVKK: Referring to the Accountability section of Table 1, Turkey could strengthen KVKK's effectiveness by adopting independent auditing systems and stricter accountability measures similar to GDPR.

Clarifying Proportionality and Relevance: The Relevance, Limited Scope, and Proportionality row of Table 1 highlights a need for clearer definitions in KVKK. This would help reduce the potential for exceptions being misused or applied inconsistently.

These insights drawn from Table 1 demonstrate the potential for aligning KVKK more closely with GDPR to ensure a more robust data protection framework in Turkey.

In the United States, there is no federal law that fully corresponds to the GDPR. However, some state laws have introduced regulations similar to the GDPR. Specifically, California's California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), Virginia's Virginia Consumer Data Protection Act (VCDPA), and Colorado's Colorado Privacy Act (CPA) provide protections akin to the GDPR.

These state laws grant consumers more rights in personal data processing while imposing responsibilities on businesses regarding data management and transparency. For instance, CCPA

and CPRA give consumers the right to delete data and opt-out of data sales, while requiring businesses to maintain transparency in their data processing practices. Similarly, VCDPA and CPA include regulations on personal data processing, data subjects' rights to consent and objection, data access, and correction.

When the U.S.'s reference regulations and the European Union's GDPR are evaluated together, it becomes clear that the fundamental principles of KVKK regarding the processing of personal data have gained a universal and international character. This demonstrates that regulations in the field of personal data protection are shaped globally around similar principles, and all regulatory frameworks share a common goal of protecting individuals' privacy. Both U.S. state laws and the GDPR emphasize principles such as data minimization, data subjects' rights, and data security, which are in harmony with the general principles of KVKK. (California Legislature, 2018)

2.4. KVKK Article # 6

Article 6 of the law, as a rule, prohibits the processing of sensitive personal data. However, it allows for certain exceptions under very specific conditions. For example, if the data subject has made the data public or if the data needs to be processed in matters threatening public health, it may be allowed, but only by specifically authorized individuals and within the limits of the relevant issue. When the article study was first initiated, reports surfaced suggesting that during the pandemic, which affected both our country and the world in recent years, there were allegations that personal data might have been leaked through the healthcare system. These claims (BBC, 2023) have heightened concerns about data security and privacy. Later on, these allegations did not subside but instead continued to grow and intensify. The responses from authorities on this issue, rather than alleviating doubts, have further increased concerns.

2.5. Exceptions of KVKK

The Personal Data Protection Law No. 6698 (KVKK) establishes comprehensive rules and principles to ensure the protection of personal data. However, in certain situations, some provisions of this law may not apply. The exceptions outlined in Article 28 of the law provide exemptions from the obligations imposed by the law under specific conditions. Here are the exceptions of KVKK;

Scientific, Historical, Literary, or Artistic Purposes: When personal data is processed for scientific research, historical studies, literary works, or artistic activities, such processing may be exempt from certain provisions of the law. This exception is intended to promote freedom of expression and academic work.

National Defense, National Security, Public Safety, Public Order, or Economic Security Purposes: Data processing activities related to critical matters such as national defense, national security, public safety, public order, or economic security are also among the exceptions of the law. In these cases, data processing may be necessary for the safety of the state and society, and such activities may be exempt from certain data protection obligations.

Prevention of Crimes or Criminal Investigations: The processing of personal data for the prevention of crimes or for criminal investigations may be exempt from certain provisions of the

law. This exception is necessary to ensure justice and to conduct effective investigations into crimes.

The Personal Data Made Public by the Data Subject: Personal data made public by the data subject may not be subject to certain provisions of this law. Data that a person voluntarily makes public can be processed more broadly.

Processing of Personal Data for the Execution of Oversight or Regulatory Duties by Public Institutions and Organizations: The processing of personal data within the scope of oversight or regulatory duties carried out by authorized and competent public institutions and organizations may be exempt from certain provisions of the law. This exemption is introduced to ensure the effective functioning of public order and control mechanisms.

2.6. Compliance of Exceptions With General Principles

The exceptions specified in Article 28 of the KVKK (Personal Data Protection Law) indicate that certain provisions of the law will not apply under specific circumstances. However, these exceptions do not completely eliminate the obligation to comply with the general principles of data processing. Even in exceptional situations, data processing activities must be carried out in a manner that is legal, fair, transparent, and consistent with the purpose. "*The thing that is exempted must be smaller than the thing that is not exempted, for the exemption to have any meaning. Moreover, even if the scope is narrowed after the exemption, the general provision must still be applicable. Otherwise, the general rule disappears; the exception becomes the general rule.*" (Gözler, 2012)

In this article, the necessity of ensuring the compliance of exemption provisions with general principles and the issues that may arise in case of violation of these principles are discussed with concrete examples and cases. Specifically, how the compliance of data processing activities with general principles should be ensured in critical areas such as public safety and economic security is demonstrated through official documents and court records.

KVKK (Personal Data Protection Law) establishes comprehensive principles and rules to ensure the protection of personal data, while also defining exceptions that will not apply in certain situations. However, these exceptions do not eliminate the obligation to comply with the general principles. Therefore, even data processing activities within the scope of exceptions must be carried out in a lawful, transparent, and purpose-compliant manner. Our article explains the attention and care required to achieve this balance with concrete examples.

2.7. Institutions Authorized To Apply For Exemption and Collect Intelligence

General Directorate of Security (EGM): Carries out intelligence activities to ensure public order and prevent crimes. Relevant Law: Police Duty and Authority Law No. 2559. EGM collects this data under the provision of Article 7 of PVSK Appendix. However, there is an obligation to comply with the additional provisions added in 2005. Additionally, the responsibility for collecting this data is assigned to the Intelligence Department.

General Command of Gendarmerie: Carries out intelligence activities to ensure security in rural areas. Relevant Law: Under Article 7 of the Gendarmerie Organization, Duties, and Powers Law No. 2803, it is authorized to collect intelligence.

Financial Crimes Investigation Board (MASAK): Collects intelligence to combat money laundering and the financing of terrorism. Relevant Law: Law No. 5549 on the Prevention of Laundering Proceeds of Crime. MASAK primarily collects and monitors this data to track suspicious transactions. However, it is also evident from Articles 6 and 7 of Law No. 5549 that there are no restrictions or limitations on the collection of these data.

National Intelligence Organization (MİT): The primary agency responsible for Turkey's foreign and domestic intelligence activities. Relevant Law: State Intelligence Services and National Intelligence Organization Law No. 2937. MİT does not present this data to courts. It is only required to provide intelligence data concerning espionage activities.

"*Except for espionage and crimes against state secrets, the use of information collected by the National Intelligence Organization (MİT) as evidence is unlawful. The only way MİT's reports can be considered as evidence is in cases falling within the scope of Article 1/1 of the supplementary article of the State Intelligence Services and National Intelligence Organization Law No. 2937. According to this article, 'Intelligence-related information, documents, data, and records under the control of the National Intelligence Organization, as well as analyses conducted, cannot be requested by judicial authorities, except for crimes listed in Chapter 4, Section 7 of the Turkish Penal Code, Articles 326 to 339, which include espionage and crimes against state secrets.' Except for these crimes, intelligence-related information, documents, data, records, and analyses collected by MİT cannot be used as evidence in trials.*"[8] (Şen & Efe, 2024).

In this way, it is clear that the law allows data collection within this scope by utilizing its exceptions. However, among the examples obtained in this study, there is no case from MİT reflected in court records, and in light of the above information, this is not possible. However, data collection activities are observed under the exceptions of the KVKK with respect to other institutions, particularly in areas of terrorism by the General Directorate of Security (EGM) and in financial matters by MASAK.

Data processing of information collected during intelligence activities must be carried out in accordance with the general principles set by KVKK and other relevant regulations. These principles and regulations ensure the protection and processing of personal data, safeguarding individuals' fundamental rights and freedoms. Compliance with these rules in all data processing activities, including exceptional circumstances, is of critical importance for ensuring data security and privacy (Atlı, 2019).

2.8. Other Legislation That Must Be Complied With Alongside General Principles

Even within the scope of exceptions, compliance with general principles is mandatory. According to Article 4 of the law, compliance with other laws is also required. The Constitution is at the

[8] Şen, E., & Efe, E. (2024, January 15). İstihbari bilgilerin tutanağa bağlanması ve ihbarcının duruşmada dinlenmesi. Ersan Şen Hukuk ve Danışmanlık. Link: https://sen.av.tr/tr/makale/istihbari-bilgilerin-tutanaga-baglanmasi-ve-ihbarcinin-durusmada-dinlenmesi

forefront of these laws. Article 20 of the Constitution and Article 15, Paragraph 2 of the European Convention on Human Rights (ECHR), which prohibits opinion research, regulate the protection of personal data.

Additionally, the Turkish Penal Code (TCK) regulations regarding the confidentiality of investigations (Article 285), the illegal acquisition of data (Article 136), its publication (Article 137), and its acquisition (Article 138); the additional provisions of the Police Duty and Authority Law (PVSK) Article 7; the Law No. 298 on the Basic Provisions of Elections and Voter Registers; the Law No. 5809 on Electronic Communications; Law No. 5549 on the Prevention of Laundering Proceeds of Crime (MASAK Law); and Law No. 5411 on Banking (BDDK Law) also require compliance with these laws and general principles, even in cases that fall under the exceptions to the KVKK provisions.

If we look closer to Table 2, it becomes evident that compliance with both the general principles of the law and other regulations under KVKK exceptions is not optional, but a necessity that protects society as a whole. In a place governed by normative law, adherence to the highest norms-namely the provisions and limitations of the Convention and the Constitution-is required. Furthermore, it is clear that institutions benefiting from the law's exception provisions must also comply with the restrictions in their own regulations.

It seems like you're referring to a table that lists various legal regulations and relevant articles related to the protection of personal data:

Table 2. Comparison of Other Legal Provisions

Legal Regulation	Relevant Articles	Summary of Content	Relevance to KVKK Exceptions
European Convention on Human Rights (ECHR)	Article 15(2)	Prohibits the suspension of certain fundamental rights, such as freedom of thought, even during emergencies.	KVKK exceptions must respect fundamental rights outlined in ECHR, ensuring exceptions do not lead to overreach or blanket surveillance.
Constitution of Turkey	Article 20	Protects the privacy of personal and family life; personal data can only be processed with explicit consent or as provided by law.	KVKK exceptions must align with constitutional protections, ensuring individual privacy is safeguarded even in exceptional cases.
Turkish Penal Code (TPC)	Articles 136, 137, 138	Regulates unlawful acquisition, dissemination, and retention of personal data beyond its legal retention period.	Any data processing under KVKK exceptions must adhere to these penal provisions to avoid violations such as unlawful retention or dissemination of data.
Police Duty and Authority Law (PVSK)	Article 7 (Appendix)	Authorizes intelligence data collection with judicial oversight; additional amendments require compliance with data protection principles.	KVKK exceptions for public safety must comply with PVSK's judicial oversight and limitations to prevent misuse of data collection powers.
Law on the Prevention of Laundering Proceeds of Crime (MASAK Law)	Articles 6, 7	Requires continuous reporting and sharing of financial data for combating money laundering and financing terrorism.	Exceptions under KVKK for financial crime investigations must ensure proportionality and data minimization, even when fulfilling MASAK obligations.
Law on Banking (BDDK Law)	General Provisions	Ensures the confidentiality and protection of personal data in the banking sector, limiting data processing to specific purposes.	Financial institutions must align their data processing practices under KVKK exceptions with the confidentiality principles outlined in BDDK Law.
Electronic Communications Law	General Provisions	Mandates the protection and confidentiality of personal data in electronic communications.	Any exception under KVKK involving communication data must follow these confidentiality requirements to protect user data.
Election Law (Law No. 298)	Voter Data Protection Provisions	Regulates the use and sharing of voter data, restricting its distribution to qualified political parties only.	Exceptions involving voter data under KVKK must not violate the limitations set by election laws to prevent misuse of sensitive voter information.

Source: Prepared by the authors based on their analysis.

As highlighted in Table 2, KVKK exceptions must operate within the boundaries of other legal regulations, such as the Constitution of Turkey (Article 20) and the Turkish Penal Code (Articles

136-138). These ensure that exceptions do not infringe upon fundamental rights, such as the protection of privacy or the prohibition of unlawful data retention.

The Election Law (Law No. 298), outlined in Table 2, emphasizes the restricted use of voter data, limiting its sharing to political parties under specific conditions. Similarly, the Law on Banking (BDDK Law) and MASAK Law enforce strict rules for handling sensitive financial data, even when KVKK exceptions apply. These examples demonstrate the need for proportionality and purpose limitation in exception-based data processing.

As noted in the Police Duty and Authority Law (PVSK) section of Table 2 intelligence data collection is subject to judicial oversight. KVKK exceptions for public safety or national security must adhere to these additional safeguards to prevent potential misuse.

Table 2 illustrates how sector-specific regulations, such as the Electronic Communications Law, govern the confidentiality of personal data in communication activities. Any KVKK exception involving communication data must align with these provisions to maintain user trust and data integrity.

The inclusion of the European Convention on Human Rights (ECHR) in Table 2 reinforces the idea that KVKK exceptions must respect universal principles of data protection and human rights, ensuring that exceptions do not undermine constitutional and international obligations.

By referring to the legal frameworks detailed in Table 2, this analysis emphasizes the necessity of embedding KVKK exceptions into a broader system of checks and balances. This approach ensures that exceptions remain proportional, lawful, and aligned with both domestic and international standards.

Table 2 summarizes various legal regulations related to the protection of personal data and the important articles within these regulations. These articles form the legal framework for the protection of personal data, safeguarding individuals' fundamental rights and freedoms. This article is not part of other regulations but is specifically within the law itself.

The inclusion of Article 6 in Table 2 is due to the general consensus on the strict safeguards surrounding the use of sensitive personal data. This article generally prohibits sensitive personal data and only allows exceptions under very strict measures, and only in cases concerning public health. This article lies between the general principles and exceptions of the law. However, it needs to be addressed separately. This is because, in the 'Example Cases,' it has been observed that MHRS (National Healthcare Registration System) data was used as intelligence data. In these examples, the source of the data is shown as MHRS, but there is no explanation about data minimization, such as whether diagnostic information or prescription details were not taken from or present in this data pool. Similarly, there is no explanation for examination data either (Example Cases, 2022-2024).

2.9. Manipulative Data Use and Data Integrity Issues

Manipulative data use refers to the alteration or use of data in a way that is not aligned with its intended purpose. This can severely impact the reliability and accuracy of the data. Manipulative data use can occur in the following ways;

Misinterpretation of Data: Data taken out of context or misinterpreted can lead to misleading conclusions. For example, if a person's financial transactions are evaluated based on only a specific period, it may create a false impression of that person's financial situation

Intentional Alteration of Data: In some cases, data is intentionally altered or manipulated. This is particularly seen in data analysis for criminal investigations or political purposes. Manipulated data can lead to wrong decisions and cause innocent individuals to be unfairly accused.

Data Taken Out of Context: Ignoring the context in which the data was collected can lead to incorrect conclusions. For example, a person's online shopping data may be used to make broad inferences, even though it does not reflect all of their habits.

Data Integrity Issues: Data integrity refers to maintaining the accuracy, consistency, and reliability of data. Data integrity issues include:

Data Corruption: Technical errors that occur during the storage or transmission of data can lead to data corruption. This is particularly common in outdated or insecure data storage systems.

Challenges in Ensuring Data Accuracy: Failure to update or verify the accuracy of data can lead to decisions based on incorrect information. For example, if a health records system lacks up-to-date health information about patients, incorrect treatments may be administered.

Unauthorized Access and Data Manipulation: Unauthorized access to data can lead to its unauthorized alteration or deletion. This is a common issue in systems where data security measures are insufficient.

2.10. Positive Developments in the Protection of Personal Data

Annulment of the Presidential Decree (CBK) on MASAK’s Duties Regarding Personal Data by the Constitutional Court:

The Constitutional Court (AYM) annulled the section of the Presidential Decree (CBK) regulating the duties of the Financial Crimes Investigation Board (MASAK) concerning personal data. The AYM ruled that the fundamental principles governing the processing and protection of personal data must be determined by law, emphasizing that the regulation introduced through the CBK violated Articles 13 and 20 of the Constitution. The court stated that the protection of personal data is a fundamental right and that such regulations must be enacted by the legislative body, namely the Grand National Assembly of Turkey (TBMM). This decision clearly establishes that the executive branch cannot unilaterally regulate the processing of personal data, and that the will of the legislature must be prioritized in this regard.

Annulment of the Security Investigation Law Enacted During the State of Emergency by the Constitutional Court on Grounds of Personal Data Protection:

The Security Investigation and Archive Research Law, enacted during the State of Emergency (OHAL), introduced a comprehensive investigation mechanism for individuals applying for public office. However, due to the lack of explicit legal safeguards in the collection, processing, and sharing of personal data, the Constitutional Court annulled the law. In its ruling, the AYM emphasized that the principles of clarity and foreseeability must be upheld in personal data processing and that such procedures must be based on a clear legal framework to prevent arbitrariness. Furthermore, the court ruled that security investigations constitute an interference with the right to personal data protection and that such interference must be justified by a clear and specific legal basis. This ruling highlights the necessity of strict oversight in security investigations related to personal data to ensure compliance with data protection laws (Barın & Uslu, 2024).

Evaluation of the 7315 Security Investigation and Archive Research Law and Its Regulation in Terms of Personal Data Safeguards:

The 7315 Security Investigation and Archive Research Law and its corresponding regulation provide significant safeguards for the protection of personal data. Under this framework, personal data obtained during security investigations and archive research must be deleted or destroyed once the purpose of processing is no longer valid or within a maximum period of two years. This provision aligns with the fundamental principles of the Personal Data Protection Law (KVKK) No. 6698, such as data minimization, purpose limitation, and proportionality. As a result, this law prevents the unnecessary and indefinite retention of personal data, ensuring that individual privacy rights are upheld and data security is maintained. In this regard, the 7315 Law and its associated regulation demonstrate compliance with the spirit and essence of KVKK, establishing a balanced approach between public security and individual data privacy (Akkaş & Doğan, 2023).

3. CASE STUDIES AND DISCUSSIONS

Case studies are real and actual events. They consist of the examination of two reports, four official letters, and one protocol, all submitted to administrative courts and obtained with the consent of the data subjects, with the specified dates and numbers. Additionally, references are made to one communication with the Energy Market Regulatory Authority (EPDK) and one with CİMER (Communication Center of the Turkish Government) aimed at correcting incorrect information in the reports.

The official letters, reports, and protocols obtained are much more extensive. However, each selected and examined example has its own unique characteristic. None of the events are related to a criminal investigation

Report 1

This report, prepared and sent by the General Directorate of Security (EGM), includes an analysis of all social media activity of an individual and all members of their family. It even reflects the

attempt to break into well-known social media platforms using password cracking techniques. A specific selection of posts from the individual was made, and their opinions and worldview were investigated. The phrase 'a password reset inquiry was made' used in the report revealed the rights that the law enforcement believes it possesses.

Report 2

This report, prepared and sent by the General Directorate of Security (EGM), contains digital records of a real individual covering all periods where data was collected and available. These include records from the Supreme Election Council (YSK), ÖSYM, Energy-Water-Natural Gas subscriptions, all telephone subscriptions and HTS (Call Data Records), MHRS data, internet shopping, pizza and hamburger orders, first, second, and third-degree relatives, and even data on consanguineous relatives.

The relevant individual questioned the authority under which this data was collected through a CİMER application, and the response indicated that it was done under the authority specified in Article 7 of PVSK (Police Duty and Authority Law) Appendix. (CİMER 1, 2024)

However, according to the relevant article and additional provisions, the authority to collect such data lies with the Intelligence Department, not the department that prepared the report. Furthermore, it was stated that the data was obtained under the instruction of the prosecutor's office. Prosecutors, however, are not authorized to collect such data or issue orders to collect it.

Such large-scale data (meta-data) can only be collected with a court order, as clearly outlined in other regulations. Additionally, it is explicitly mentioned in the report that the data cannot be trusted and has been manipulated. The use of the phrase 'modified by the presidency' actually indicates an attempt to standardize the format. However, a simple examination reveals that the data format changes constantly throughout the report. This clearly indicates that the data was manually processed.

For instance, in the example cases, the data was manipulated by the relevant department, and even if it was not intentional, the manually performed actions changed the results. The individual was able to prove that the data did not belong to them as a result of correspondence with the energy company. (EPDK, 2024) However, it is not always possible to easily access the truth of the information in this way. Some data cannot be verified because, in certain cases, the data is not available to anyone. In other words, data that is not even available to the institution holding it is presented by law enforcement in a format requested for court submission. In some cases, data that has been deleted or destroyed by the institutions where it was obtained is used.

For example, the HTS record retention period for the relevant company is a maximum of 10 years for invoices and 2 years for HTS details. However, law enforcement keeps these records for much longer and presents them to the courts. Considering the manual adjustments made to turn information from different data sets into a single data table, it can be understood that even without malicious intent, negligence or fault by a law enforcement officer could subject the individual to years of legal proceedings.

The collection of health data violates Article 6 of the law, which prohibits the processing of sensitive personal data. According to this provision, processing such data should be highly restricted.

The retention of YSK voter registration data, including records from previous decades, contradicts the principle that this data should only be shared with political parties participating in the election.

Examining examination data also falls under the category of sensitive personal data. Unless individuals disclose it themselves, this data is part of their privacy.

The Ministry of Finance's access to e-archive invoices, which control all trade in the country, introduces the issue of mass surveillance.

Including third-degree relatives in the investigations shows that the scope of data collection is being expanded, and the limitations should be reviewed more carefully.

Official Letter 1

This letter, prepared and sent by MASAK (Financial Crimes Investigation Board), contains all data related to the banking transactions of a real individual, covering all periods possible, including all transactions to and from all banks. Moreover, some of the data does not belong to this individual. It can be said that no fundamental principle of the law has been respected in terms of the general principles. In fact, the privilege granted for detecting suspicious transactions, regardless of the size or age of the transactions, is an issue in itself, especially when such data is stored in an insecure database without data integrity, creating a general surveillance problem. Furthermore, it is clear from the expressions used that the queries were made both online from the relevant banks and from their own archives.

When preparing the report, data was shared that did not align with the request of the relevant judicial unit. The relevant judicial authority only asked whether a report had been prepared on a specific topic, and after MASAK stated that such a report did not exist, it sent its unlimited data to the judicial authorities, believing it might be useful.

However, the main issue here is the use of the Turkish Citizenship Number (TCKN), even in periods when it did not exist. The report itself acknowledged at the beginning that there may be some omissions and errors.

The issues in the report do not stop there: The individual for whom the report was prepared has bank accounts and account activity in banks where they never held an account. This suggests that the system not only contains errors but also has the potential to falsely attribute actions to individuals. The system used to prepare the report has proven unreliable, and its failure to produce accurate data has only caused confusion for the authorities who did not request such data but could have obtained the most up-to-date data legally if they needed it.

The fact that these data were held as intelligence data does not make them legally valid. The individual questioned through CİMER how these data, which did not belong to them, were obtained. The response received was that the data could not be disclosed due to the "state secrecy" prohibition. (CİMER 2, 2024) In reality, the individual's personal secrets have been exposed, but the explanation given was that these secrets belong to the state.

Official Letter 2

This letter, prepared and sent by MASAK (Financial Crimes Investigation Board), contains all data related to the banking transactions of a real individual, covering all periods possible, including all transactions to and from all banks. This is the second incident, demonstrating that the previous event was not a one-time occurrence but rather a repeated and non-coincidental event.

Official Letter 3

In the data analysis prepared and sent by EGM (General Directorate of Security), this individual has been kept under suspicion based on a short, one-time phone call made 13 years ago using a phone that they were not the sole user of. The report indicates that it should be considered that the previous or subsequent owner of the phone might have been mixed up. Despite the expression in the report stating "the subscriber's T.C. Identity Number is not available," the TCKN number used is a clear indication of manual tampering. In this particular case, the individual is neither the owner of the phone nor the user, yet significant conclusions have been drawn from a single trace.

Official Letter 4

In the data analysis prepared and sent by EGM (General Directorate of Security), the report mentions phrases such as "there may be date discrepancies, records may be corrupted," yet data that cannot be trusted to this extent is presented in tables as if they were definitive evidence, which could be considered as traces or indications by the investigative authorities. In other words, it seems that even the authors of the report are implicitly saying "don't trust too much..." but still present this data to the courts as though it were conclusive evidence. In summary, based on this document, it appears that TCKN (Turkish Citizenship Number) records from periods when TCKN did not exist were manually supplemented with TCKN obtained from another source.

Minutes

In the minutes prepared and sent by EGM (General Directorate of Security), the phrase "by reviewing all the statement records nationwide" clearly indicates that the extent of the investigation is nationwide. An officer who is conducting research or an investigation on an individual can conduct a nationwide inquiry.

3.1. Evaluation of Case Studies

Exceptions introduced by Article 28 of the KVKK (Personal Data Protection Law) provide exemptions from the obligations of personal data protection in certain situations. However, these exceptions do not completely eliminate the obligation to comply with the general principles. Even in exceptional cases, data processing activities must be carried out in a lawful, fair, transparent, and purpose-compliant manner. There is no need for additional regulations or explanations to understand this.

Table 3. Legal Evaluation and Compliance of Case Studies under KVKK Exceptions

Case	Applicable Laws Beyond KVKK	Was the Data Collection Method Lawful?	Are the Provided Data Reliable, Accurate, and Up-to-Date?	Does It Comply with Purpose Limitation and Data Minimization Principles?
Report 1: Social Media Monitoring	ECHR Article 15(2)	No explicit violations noted; however, the nature of the data collection could indicate breaches in proportionality and relevance.	Data is current, but the scope is overly broad, including unnecessary details about family members' activities.	Violates minimization principles by collecting all social media activity, including non-relevant and private data of family members.
Report 2: Comprehensive Personal Data	Turkish Constitution Article 20, Election Law (YSK), Turkish Penal Code (TPC)	Violates PVSK Appendix 7 by collecting data beyond permitted authority; unauthorized inclusion of voter records and private details.	Data is outdated and includes irrelevant information such as historical voter records, unrelated financial transactions, and even food orders (e.g., pizza).	Breaches purpose limitation by including excessive, irrelevant data; minimization principles are entirely ignored.
Official Letter 1 (MASAK)	Banking Law (BDDK), MASAK Law Articles 6-7	Data collected as part of intelligence activities but lacks judicial oversight, violating procedural safeguards.	Acknowledged inaccuracies in the letter; includes erroneous financial data from unrelated individuals.	Provides unlimited financial data without filtering for relevance, directly breaching data minimization principles.
Official Letter 2 (MASAK)	Banking Law (BDDK), MASAK Law Articles 6-7	Same issues as Official Letter 1: lacks judicial oversight and procedural safeguards.	Same inaccuracies as in Official Letter 1; financial data contains errors and unrelated records.	Continues the trend of collecting and sharing excessive data without proportionality or relevance safeguards.
Official Letter 3 (EGM)	Turkish Penal Code Article 135, PVSK Appendix 7	Violates lawful collection practices by associating individuals with phones they neither own nor use, without verifying the data.	Data has been manipulated to link a person to activities unrelated to them, undermining reliability and trustworthiness.	Fails to apply minimization or proportionality principles; irrelevant data included without proper validation or justification.
Official Letter 4 (EGM)	Turkish Penal Code Articles 135, 285	Violates investigation confidentiality by sharing unreliable data in its reports.	Explicitly admits inaccuracies, with manipulated or inconsistent data formats used in the report.	Provides data with no minimization efforts; the shared information exceeds what was necessary or lawful for the investigation.
Minutes (EGM Nationwide Search)	Turkish Penal Code Articles 135, 285	Violates investigation confidentiality; nationwide search exceeds lawful scope and includes irrelevant and non-targeted data.	No data provided, indicating a lack of accuracy and accountability.	Fails minimization and proportionality; a blanket collection of all data, regardless of relevance, is incompatible with data protection principles.

Source: Prepared by the authors based on their analysis.

Compliance of Exception Provisions with General Principles: Compliance of exception provisions with general principles must be ensured. Exceptions require that data processing activities be carried out in accordance with their intended purpose and that the fundamental principles of personal data protection are not violated. For example, even in data processing activities carried out for reasons of national security or public order, it is essential that the data is processed accurately, up-to-date, and securely.

Issues in the Application of Exceptions: One of the biggest issues in the application of exceptions is the failure to evaluate these situations in compliance with general principles and the broad application of exception provisions, which has led to difficulties with general surveillance practices. For example, MASAK's broad and continuous collection of data related to banking transactions contradicts the principle of data minimization. Similarly, the broad collection of personal data by EGM without a specific purpose violates the principles of legality and proportionality.

Incorrect Application of Exceptions Should not Lead to General Surveillance

The most significant issue in the application of KVKK (Personal Data Protection Law) in Turkey, as shown by the case studies, is the arbitrary use of exception provisions, which has almost turned this practice into "General Surveillance".

It appears that EGM (General Directorate of Security) has collected data on all individuals, regardless of whether they are under investigation, by engaging in opinion research, which is considered a core right. This includes social media, all commercial and economic activities, all banking transactions, exam data, health records, voter information, and phone calls, without regard to size, age, or relevance, stored in a single database. In doing so, EGM does not comply with the additional provisions added in 2005 to its own working law, PVSK Appendix 7. The principles of purpose limitation, proportionality, and data minimization are also violated. Furthermore, although the Intelligence Department should be the authorized unit for collecting and processing these data, it is evident that other departments have been using this authority. Additionally, while intelligence data intended for preventive purposes can be obtained through judicial orders and verified using external methods, it seems that this path was not pursued, likely due to workload considerations.

Similarly, MASAK (Financial Crimes Investigation Board) appears to have collected all data about individuals, without distinction between old or new, suspicious or not, large or small, and shared this data under the guise of intelligence with unrelated authorities, while being aware that the data is neither accurate nor reliable. Moreover, like the example from the police, intelligence data, which should be used for preventive purposes, could have been verified through judicial orders but was likely not pursued for reasons related to workload.

The practices of these two institutions, which benefited from the exceptions of the law, reveal that the vast authority used by these institutions resulted in the violation of the general principles of this law, along with the conditions for processing all special categories of data listed in Article 6, and the processing conditions of citizens' confidential data according to all regulations.

At the end of 2022, the investigation into a politically motivated murder and the mafia operations conducted by the new government established after the 2023 Turkish general elections raised serious concerns in society about the use of personal data. These events revealed that the vast amount of data collected by EGM and MASAK is at risk of being exploited by malicious actors due to significant security flaws. What makes this situation even more troubling is the revelation that the individuals responsible for safeguarding this data are, in fact, the very people expected to combat such threats (T24, 2024).

Security flaws have been observed in the processes of data collection, use, and monitoring. Another consequence of the unlimited collection of electronic and digital data of an individual or society is that if this data falls into the hands of criminal organizations, the potential negative outcomes for individuals could be limitless. Not only those under criminal investigation, but also the general public's phone, banking, and commercial activities are shared without ensuring data integrity and protection, which resembles Jeremy Bentham's "Panopticon" model. The Panopticon refers to a system where individuals feel they are constantly under surveillance, thus controlling their own behavior (Bentham, 1791). In the digital age, this system, where individuals' data is constantly monitored, manifests itself as a similar mechanism of surveillance and control in modern societies (Foucault, 1975).

In 2014, the European Court of Justice annulled the 2006 EU Directive, arguing that it violated individuals' fundamental rights. This directive had required communication companies to store traffic and location data. The decision stated that the indiscriminate and blanket collection of data was incompatible with individual privacy rights at the EU level.

The European Court of Justice's (ECJ) ruling on the annulment of mass surveillance includes a series of decisions that prohibit blanket data collection by member states that do not comply with data protection laws. These rulings emphasize that the extensive collection and storage of personal data are contrary to the fundamental rights of the European Union (EU).

In the years following this decision, the ECJ similarly extended its rulings to include the laws of member states. For example, in 2017, in the cases of Tele2Sverige and Watson, the court ruled that the indiscriminate and blanket collection of data by member states was illegal. The ECJ also stated that large-scale data collection for national security reasons must comply with EU privacy laws (Court of Justice of the European Union, 2016).

These rulings led many EU member states to reassess their surveillance practices. However, despite these decisions, some countries continued to collect data using different methods. For instance, France defended its large-scale data collection practices by citing a constant terrorist threat (Propp, 2020).

These decisions are seen as an important step in protecting individual privacy rights in the EU and represent a strong stance against mass surveillance practices.

Mass surveillance turns a country into a Panopticon (Bentham, 1791). Mass surveillance is not only harmful; it also complicates matters and makes them inextricable. It is like being able to see all ten thousand people in the opposite stand during a football match, but not seeing any of them at all. Considering the unlimited data tracking, the scale of the personnel needed to make sense

of it must also be taken into account. However, if limited to the purpose and with data minimization in mind, this legal economy will help reduce or even eliminate the potential for harm caused by confusion, omissions, and errors.

3.2. Discussions

This section evaluates the challenges in balancing the exception provisions of KVKK with its general principles and explores their broader implications for data protection practices in Turkey.

Balancing Security and Privacy: While exceptions under KVKK aim to address critical areas such as public security and economic stability, their broad application often leads to significant privacy concerns. For example, the practices of MASAK and EGM demonstrate that the principles of data minimization and proportionality are frequently violated. This raises the question: how can public institutions achieve their goals without undermining the fundamental rights of individuals?

The Role of Oversight Mechanisms: The absence of robust oversight mechanisms is a recurring issue. Regular audits and transparency reports could help ensure that exception provisions are not misused as tools for mass surveillance. Lessons can be drawn from the GDPR's strict accountability framework.

Implications of International Comparisons: The GDPR's emphasis on transparency and proportionality contrasts with KVKK's loose enforcement of similar principles. Although KVKK aligns with GDPR in theory, its practical application highlights a gap in implementation. This discrepancy highlights the need for Turkey to adopt more rigorous enforcement practices.

Mitigating the Risk of General Surveillance: The unchecked use of exception provisions risks turning Turkey's data protection regime into a Panopticon-like system. By narrowing the scope of exceptions and ensuring compliance with general principles, Turkey can strike a better balance between security and individual privacy.

Future Directions: To prevent the misuse of exceptions, policymakers should consider strengthening KVKK by introducing clearer guidelines for the application of exceptions, enhancing inter-institutional collaboration, and fostering a culture of data protection awareness.

4. Conclusion and Recommendations

4.1. Conclusion

The Personal Data Protection Law (KVKK) No. 6698 is designed to protect individuals' fundamental rights and freedoms during the processing of personal data and to determine the obligations of data controllers. However, Article 28 of the law defines certain exceptions. While these exceptions provide exemptions from personal data processing obligations in certain situations, they do not completely eliminate the need to comply with general principles. This article examines the challenges in ensuring compliance with general principles in the application of exception provisions, with concrete examples and cases. The broad application of exception provisions has been evaluated in terms of data minimization and purpose limitation principles.

General Principles and the Application of Exceptions: Article 4 of KVKK sets out the general principles for data processing activities, requiring them to comply with the law, fairness,

transparency, the principle of data minimization, and purpose limitation. Even data processing activities based on exception provisions must comply with these general principles.

4.2. Recommendations

Strengthening Audit Mechanisms: Independent auditing bodies should regularly check and report on the compliance of data processing processes under exceptions with general principles. These audits should include both internal and external audit processes, and the results should be publicly shared. Furthermore, any non-compliance in data processing activities should be quickly corrected, and responsible individuals should be subject to penalties. This is critical to prevent the misuse of exception provisions.

Increasing Transparency of Data Processing Procedures: Relevant institutions should disclose their data processing processes and how these processes are managed to the public. This transparency is important for protecting data subjects' rights. Additionally, data sharing between institutions, particularly under exception provisions, should be governed by clear rules, and these processes should be regularly audited. Each institution should prepare annual reports on their data processing activities, which should be publicly available.

Training and Raising Awareness: Public institutions and the private sector should become more aware of data protection. Regular training on the general principles and exceptions of KVKK should be provided. These trainings should not be limited to theoretical knowledge, but also focus on practical examples of data processing processes, highlighting key considerations. In addition to this training, internal awareness campaigns should be organized, and employees should be encouraged to take responsibility in this area.

Strengthening Legal Regulations: Existing legal regulations should be reviewed and strengthened if necessary. Mechanisms to prevent the misuse of exception provisions should be established, and these mechanisms should be regularly audited. Additionally, the principle of proportionality in inter-institutional data sharing should be ensured, and the principle of data minimization should be applied more strictly. In the event of an infringement, a swift sanction mechanism should be implemented, and responsibilities should be clearly defined.

Strengthening Inter-Institutional Cooperation: Cooperation between institutions is a critical element in increasing transparency and compliance in data processing activities. All relevant institutions should establish common standards for data processing activities and hold regular meetings to ensure compliance with these standards. These cooperation processes will enhance data security and protection measures, preventing the misuse of exceptions.

Data sharing processes under the exception provisions should be based on clearer and more transparent rules between institutions. It is recommended that these processes be monitored and reported by independent auditing bodies.

Even data processing activities carried out under the exception provisions of KVKK must comply with the general principles. Ensuring compliance with these principles is critical for the protection of personal data. The examples discussed in this article highlight the necessity of applying exception provisions in a manner that is consistent with general principles. Transparent

mechanisms and regular audits aimed at achieving this balance are recommended for future regulations.

REFERENCES

Aşıkoğlu, Ş. İ. (2019). Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-. Kişisel Verileri Koruma Dergisi, 1(2), 41-65.

Akkaş, A. H., & Doğan, N. (2023). YARGI KARARLARINDA GÜVENLİK SORUŞTURMASI VE ARŞİV ARAŞTIRMASI. Adalet Dergisi, (71), 853-878.

Atlı, T. (2019). Kişisel verilerin önleyici, koruyucu ve istihbari faaliyetler amacıyla işlenmesi. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 2*(1), 4-22.

Aydın, İ. (2024). AİHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması. Firat University Journal of Social Sciences, 34(1), 217-235.

Barın, T., & Uslu, M. T. (2024). ANAYASA MAHKEMESİNİN İPTAL KARARLARININ YÜRÜRLÜĞÜNÜN ERTELENMESİ KURUMU VE CUMHURBAŞKANLIĞI KARARNAMELERİNDE GÖRÜNÜMÜ. Türkiye Adalet Akademisi Dergisi, (59), 51-90.

Bentham, J. (1791). *Panopticon: or, The Inspection-House*.

Bertoni, E. (2021). Convention 108 and the GDPR: Trends and perspectives in Latin America. Comput. Law Secur. Rev., 40, 105516.

California Legislature. (2018). *California Consumer Privacy Act (CCPA) of 2018*.

Council of Europe. (1981). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).

Court of Justice of the European Union. (2016, December 21). Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others (Joined Cases C-203/15 and C-698/15). EUR-Lex.

Çubukcu, Z. (2024). Dijital çağda kişisel verilerin korunmasında veri koruma otoritelerinin rolü. *Toplum, Ekonomi ve Yönetim Dergisi (Journal of Society, Economics and Management)*, *5*(3), 455.

Foucault, M. (1975). *Discipline and Punish: The Birth of the Prison*.

Gözler, K. (2012, Eylül 29). Hukuk Yorum İlkeleri. Kamu Hukukçuları Platformu ve Türkiye Barolar Birliği tarafından düzenlenen "Anayasa Hukukunda Yorum ve Norm Somutlaşması" toplantısında sunulan bildiri, Ankara.

Işık, O. (2022). Kişisel verilerin korunması kanunu kapsamında veri sorumlusu olarak sosyal güvenlik kurumu. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 17*(2), 263-362.

Kaya, İ. S., & Tolun, Y. (2020). Uygulayıcılar için Türkiye'de ve Avrupa'da kişisel verilerin işlenmesi KVKK-GDPR karşılaştırması. Kitap. Ankara: *Adalet Yayınevi*.

Kişisel Verileri Koruma Kurumu. *KVKK Madde 4 - Genel İlkeler*. Retrieved June 20, 2024, from https://www.kvkkarar.com/kvkk-madde-04/

Nitelikli Veri. *Kişisel Verilerin Korunması ile İlgili Temel Bilgiler*. Nitelikli Veri. https://nitelikliveri.com

Oğuz, S. (2018). *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*. Bilgi Ekonomisi ve Yönetimi Dergisi, 13(2), 121-138.

Özkaya, Ö., & Toprak, İ. (2022). *Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi.* MANAS Sosyal Araştırmalar Dergisi, 11(3), 1291-1305.

Propp, K. (2020, February 21). Putting privacy limits on national security mass surveillance: The European Court of Justice intervenes. Atlantic Council. Retrieved June 20, 2024, from https://www.politico.eu/article/data-retention-europe-mass-surveillance/

Savaş, R. N., Zaim, A. H., & Aydın, M. A. (2020). KVKK ve GDPR Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 19(38), 208-223.

Şen, E., & Efe, E. (2024, January 15). İstihbari bilgilerin tutanağa bağlanması ve ihbarcının duruşmada dinlenmesi. Ersan Şen Hukuk ve Danışmanlık. Retrieved from https://sen.av.tr/tr/makale/istihbari-bilgilerin-tutanaga-baglanmasi-ve-ihbarcinin-durusmada-dinlenmesi

T24. (2024, June 20). Sanık Demirbaş'tan Sinan Ateş'in bilgilerini Ülkü Ocakları Başkanı'na neden gönderdin sorusuna cevap: Pankart asacaktık. T24. https://t24.com.tr/haber/sanik-demirbas-tan-sinan-ates-in-bilgilerini-ulku-ocaklari-baskani-na-neden-gonderdin-sorusuna-cevap-pankart-asacaktik,1169940

U.S. Department of Health and Human Services. (1996). *Health Insurance Portability and Accountability Act (HIPAA)*.

Yosif, U. (2021). *Kişisel Verilerin İşlenmesi Şartları Ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler.* Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, 4(1), 1-22.

Yücedağ, N. (2019). Kişisel verilerin korunması kanunu kapsamında genel ilkeler. Kişisel Verileri Koruma Dergisi, 1(1), 47-63.

DOCUMENTS REGARDING CASE STUDY (2022-2024)[9]

BBC (2023). "Türkiye'de E-Devlet verileri sızdırıldı mı? Uzmanlar endişeli" [News article]. https://www.bbc.com/turkce/articles/cn8789ez2q7o

CİMER1**.** (2024, April 22). CIMER application and response dated 22/04/2024 and numbered 2401432268.

CİMER2. (2024, May 9). CİMER application and response dated 09/05/2024 and numbered 2401629279.

EPDK : EMRA complaint and response dated 31/05/2024 and numbered -E.170595 -E.170595.

Report 1: General Directorate of Security. (2023, March 22). Report. 2023-0071238-1679468915.

Report 2: General Directorate of Security. (2023, September 21). Report. E-58604142-63044-2023092111240062092.

Official Letter 1: Financial Crimes Investigation Board. (2023). Official Letter. E-66479176-360.03.02 – 22587.

Official Letter 2: Financial Crimes Investigation Board. (2023). Official Letter. E-66479176-360.03.02 - 5967.

Official Letter 3: General Directorate of Security. (2023, May 31). Official Letter. 2023/2128.

[9] These documents are only accessible to the authors for review purposes

Official Letter 4: General Directorate of Security. (2022, September 13). Official Letter. 2022/243.

Minutes: General Directorate of Security. (2023, July 31). Protocol. 2023070621081642396.