AI-RELATED PERSONAL DATA PROCESSING UNDER THE TURKISH DATA PROTECTION LAW

Assist. Prof. Osman Gazi GÜÇLÜTÜRK*

INTRODUCTION

In the rapidly evolving landscape of technology, the integration of Artificial Intelligence (**AI**) into various sectors has brought forth complex challenges regarding the processing of personal data. The Turkish Data Protection Law[1] (**TDPL**) provides a framework of lawful grounds under which personal data can be processed; however, the applicability and adequacy of these grounds in the context of AI remain subjects of critical examination. This discourse delves into the necessity-based legal grounds outlined in Article 5(2) of the TDPL, evaluating their suitability and limitations for AI-related data processing. Furthermore, it scrutinises the role of explicit consent as a legal basis, highlighting the inherent difficulties posed by the opaque and dynamic nature of AI systems. Through a comprehensive analysis, this discussion aims to shed light on the intricate balance between facilitating technological advancement and safeguarding individual data privacy within the Turkish legal framework. In theory, AI systems do not necessarily require personal data for training purposes. For instance, they can be trained exclusively on animal images or machine-generated raw data that do not include any personal data. The composition of the dataset used to train an AI system depends on both the developer's design choices and the intended purpose of the system. However, despite this theoretical possibility, AI systems almost invariably process datasets that contain personal data to foster the advantages of modern AI systems. Virtual assistants process personal data to offer personalised assistance, while LLM-powered chatbots or downstream applications process or even generate personal data to operate according to the inputs. Processing personal data emerges as a practical necessity to implement AI systems in our daily lives in an increasing number of ways. Consequently, the rules governing personal data protection become not only relevant but also crucial.

* Galatasaray University, Faculty of Law, Department of IT Law. ogucluturk@gsu.edu.tr. This article is prepared as a part of the roundtable and article series, co-organised by Meta and Galatasaray University, and finalised after the roundtable discussion took place at Galatasaray University on 7 November 2024. All URLs in this paper are accessed on 25 November 2024, unless explicitly stated otherwise.

[1] Law No. 6698 on the Protection of Personal Data. The official Turkish version of the law can be found at https://mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5. An unofficial translation of the initial version of the law by the Turkish Data Protection Authority can be found at: https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law .

Training a model[2] is not the only stage where AI intersects with personal data protection regulations. A pre-trained model[3], regardless of whether personal data were processed during its training, may subsequently be fed personal data to generate an output. The risks associated with this process differ from those related to processing personal data during the training phase. In this scenario, the model or system may produce an output concerning the data subject rather than merely processing personal data to train the model or system. This distinction is particularly evident in the context of using AI for financial credit scoring. For example, data from previous credit decisions may be utilised to develop an AI model. This development, in isolation, may not directly impact the rights of the data subjects[4]. However, when a financial institution applies this AI model to inform its decision on whether to approve a loan for an individual—after inputting the potential borrower's information—the effect on that individual becomes unequivocal.

This article explores whether and on what grounds personal data can be lawfully processed for or by AI under Turkish law. It begins with a brief overview of the structure of the Turkish legal regime and the significance of the lawful grounds for processing personal data as stipulated by the TDPL. Based on this framework, the article first examines the compatibility of the general principles of the TDPL with AI-related personal data processing. Following this analysis, it investigates the challenges of applying the TDPL to AI-related personal data processing. The focus then shifts to identifying the appropriate lawful grounds for processing in the context of AI-related activities. The discussion is centred on two main types of AI-related data processing: processing personal data to train AI models and inputting or prompting a pre-trained model or AI system with personal data.

Before delving deeper into these issues, it is useful to clarify what is meant by AI in the context of this article. There is no universally accepted definition of AI, nor is there a consensus on whether AI requires a fixed definition[5]. This ambiguity arises not only from the dynamic nature of the field but also from conceptual differences in how AI is understood. What is clear is that modern AI systems, which have driven the recent surge in AI's popularity, operate under a different paradigm than traditional software[6]. Traditional software relies on instruction or rule-based deterministic programming, meaning that all steps required to produce an output must be explicitly coded by

[2] The term *model* refers to the software framework embodying the rules and patterns learned during the training phase. While not all AI systems are model-based, the most advanced ones almost invariably rely on such structures. For further details, see Osman G. Güçlütürk, *Yapay Zeka ve Verinin Kullanımı* (2022), p. 66 fn. 168.

[3] Pre-trained models are those that have already undergone training for specific tasks and can be seamlessly adapted for use in downstream applications. For more information on pre-trained models, see Xu Han and others, 'Pre-trained models: Past, present and future' (2021) 2 AI Open 225.

[4] For more information on using AI in credit scoring see Wilhelmina Addy and others, 'AI in credit scoring: A comprehensive review of models and predictive analytics' (2024) 18 118.

[5] For a comprehensive analysis of various definitions of AI and the discussion on whether a legal definition is necessary, see Güçlütürk, *Yapay Zeka ve Verinin Kullanımı* p. 36.

[6] For more information on this rule-based, deterministic traditional programming approach and how it differs from AI see Güçlütürk, *Yapay Zeka ve Verinin Kullanımı* p. 50.

engineers, ensuring that the same input always yields the same output. This approach, regardless of the system's complexity, provides a certain degree of transparency and predictability.

Modern AI systems[7], however, function differently. While their core code is still primarily hardcoded by humans, what is coded are not the specific steps to generate an output but rather the steps to "learn" how to produce an output. This learning process is, despite some parts of the learning architecture being inspired by the functioning of the human brain, fundamentally different from human learning; it is purely statistical based on the relationships between the provided inputs[8]. In simplified terms, modern AI systems do not receive explicit instructions to generate an output; instead, they learn these instructions from existing datasets to produce outputs similar to those in the training data[9]. Consequently, the quality and accuracy of an AI system are highly dependent on the quality of the dataset. As a result, these AI systems require vast datasets to achieve accuracy, making them significantly more pertinent to data protection laws. Therefore, this article will primarily focus on advanced and data-intensive AI systems and models.

1. LAWFUL PERSONAL DATA PROCESSING UNDER TURKISH LAW

Privacy, a multifaceted concept, is not only a broad principle but also a fundamental right enshrined in the Turkish Constitution, Article 20(3)[10]. Within Türkiye's extensive legal framework, numerous provisions address privacy concerns, including those related to the protection of personality under the Turkish Civil Code No. 4721[11] and crimes involving personal

[7] There is no universally agreed-upon definition of modern AI systems. However, for the purposes of this discussion, the term broadly refers to non-deterministic systems that infer patterns and rules from datasets to generate outputs and make decisions. These systems rely on calculations whose outcomes and processes cannot be precisely traced or predicted by humans.

[8] For more information on how learning process is conducted in machine learning in general and other specific techniques, such as deep learning or reinforcement learning differ from and compare to human learning see Niklas Kühl and others, 'Human vs. supervised machine learning: Who learns patterns faster?' (2022) 76 Cognitive Systems Research 78; Dominik Dellermann and others, 'Hybrid Intelligence' (2019) 61 Business & Information Systems Engineering 637; Been Kim and others, *Neural Networks Trained on Natural Scenes Exhibit Gestalt Closure* (2020).

[9] The challenge of drawing clear distinctions between traditional systems and AI systems, which introduce novel risks and complexities, is also reflected in legislative texts. Acknowledging the potential uncertainties arising from the adopted definition, paragraph 12 of the Recital of the EU AI Act states that "*the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data*." The official and up-to-date full text of the EU AI Act can be accessed at https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[10] Article 20(3) of the Turkish Constitution provides that *"[e]veryone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/ her personal data and being informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law*."

[11] The Turkish Civil Code (Law No. 4721) includes provisions on personality rights and their protection, which are closely linked to and encompass rights related to personal data. For more information, see Kemal Oğuzman, Özer Seliçi and Saibe Oktay-Özdemir, *Kişiler Hukuku* (Filiz Kitabevi 2018), p. 167.

data under the Turkish Criminal Code (Law No. 5237)[12]. Among these, the TDPL stands out as the primary practical legislative framework governing personal data protection in Türkiye, laying down the rules that must be respected while processing personal data and drawing from the same foundational principles as the European Union's General Data Protection Regulation (**GDPR**)[13]. Given its comprehensive scope and alignment with international standards, our analysis will focus primarily on the TDPL.

The TDPL is a law containing general provisions, and for its implementation, certain powers have been granted to the Personal Data Protection Authority ("**Authority**"). The Authority exercises these powers through the decisions of its decision-making body, the Personal Data Protection Board ("**Board**"). The Board's decisions play a crucial role in clarifying the broad expressions found in the TDPL in practice[14]. To conduct a thorough analysis, this study will reference not only the TDPL and its secondary legislation but also the guidelines issued by the Authority and the decisions rendered by the Board. Particularly significant to the central question of this study is the "Guidelines on Recommendations for the Protection of Personal Data in the Field of Artificial Intelligence,"[15] published by the Authority on September 15, 2021. Quite recently, the Authority has issued another relevant information piece titled "Information Note on Chatbots (The Example of ChatGPT)"[16].

While the TDPL does not explicitly address the processing of personal data by AI systems, this does not imply its irrelevance or non-applicability to AI-driven data processing activities. On the contrary, as the prevailing data protection legislation in Türkiye, the TDPL inherently governs all personal data processing, including that conducted by or for AI, except where specific exemptions apply. Thus, it plays a crucial role in the landscape of AI-related data processing, ensuring that personal data handling adheres to legally mandated standards of protection and privacy.

---

[12] Unlawfully obtaining, recording, and spreading personal data are tied to criminal sanctions under the Turkish Criminal Code, Articles 135, 136, and 138. For more information, see Köksal Bayraktar and others, *Özel Ceza Hukuku Cilt III: Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar* (On İki Levha Yayıncılık 2018), p. 627.

[13] The official and up-to-date full text of the GDPR can be accessed at https://eur-lex.europa.eu/eli/reg/2016/679/oj. It must be noted that the TDPL is based on the predecessor of the GDPR, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the full text of which can be accessed at https://eur-lex.europa.eu/eli/dir/1995/46/oj. On a related note, according to the annual plan of the Presidency of the Republic of Türkiye, promulgated in the Official Gazette on 30 October 2024, the harmonisation with the GDPR is planned to be completed by the end of 2025 < https://www.resmigazete.gov.tr/eskiler/2024/10/20241030M1-1.pdf>.

[14] Not all decisions of the Board are publicly accessible. Summaries of selected decisions are periodically published on the Authority's official website, www.kvkk.gov.tr. Additionally, the Board may issue decisions outlining general and foundational principles on specific topics, which are categorised as "Board Resolutions" and can be accessed directly on the Authority's website at https://www.kvkk.gov.tr/Icerik/6639/Board-Resolutions.

[15] Kişisel Verileri Koruma Kurumu, *Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence* (Kişisel Verileri Koruma Kurumu 2021). The English version of this guide can be accessed at https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/58678459-eba4-451a-a2f3-c1baf17b90f5.pdf.

[16] Kişisel Verileri Koruma Kurumu, *Sohbet Robotları (ChatGPT Örneği) Hakkında Bilgi Notu*, 2024). This note is issued only in Turkish, which can be accessed at https://kvkk.gov.tr/SharedFolderServer/CMSFiles/967c7518-2a4c-4318-9c97-01dcac2591f3.pdf.

The TDPL sets forth a series of cumulative conditions that must be met for personal data processing to be lawful:

- The processing must respect the general principles outlined in Article 4.
- The processing must be based on one of the lawful processing grounds provided exhaustively under Article 5 for non-sensitive data and under Article 6 for sensitive data.
- As per Article 7, personal data must be erased or anonymised when the conditions for lawful processing are no longer satisfied, for example, if the data subject withdraws consent.
- If personal data are to be transferred within Türkiye or to other countries, the additional rules provided under Articles 8 and 9, respectively, must be complied with.
- Pursuant to Article 10, data subjects must be informed about the processing of their personal data and about their rights as data subjects, which are provided under Article 11, before the commencement of the processing.
- As instructed by Article 12, data controllers must take necessary measures and ensure an appropriate level of data security to protect personal data and prevent unlawful access or processing.

Since these conditions are cumulative, the absence of any of them renders a personal data processing activity unlawful. In addition to these requirements, there is also an obligation for data controllers to register with the National Data Controller Registry (**VERBIS**)[17] if they meet certain criteria or engage in specific types of personal data processing activities.

Examining this detailed and complex framework of the TDPL reveals the nuanced yet critical role this legislation plays in shaping the deployment of AI under Turkish law. As we move from a broad introduction to the TDPL into a focused discussion on the general principles and their specific application to AI, it is essential to bridge these sections by considering the operational dynamics between the existing legal provisions and the burgeoning needs of AI technologies. This analysis not only contextualises the provisions of the TDPL but also prepares the ground for discussing how these regulations both facilitate and sometimes challenge the integration of AI systems into compliant data processing practices. This intermediary reflection sets the stage for a

[17] VERBIS is a publicly accessible registry available at https://verbis.kvkk.gov.tr/. As a general rule, registration with VERBIS is mandatory for all data controllers, although the Board has the authority to introduce exemptions. In addition to sector- and profession-specific exemptions, the Board has established two cumulative criteria—based on the number of employees and annual turnover—that may exempt a data controller from the registration requirement. For more information, see Ömer Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku* (On İki Levha Yayıncılık 2024), p. 219. For the decision establishing the most recent threshold see https://www.resmigazete.gov.tr/eskiler/2023/07/20230725-5.pdf.

deeper exploration of how data protection principles, while seemingly rigid, actually provide foundational flexibility, allowing for the responsible evolution of AI within the boundaries of the law.

As we conclude our brief exploration of the TDPL and its foundational role in governing personal data protection, it becomes evident that the framework establishes a robust foundation that may affect AI practices. However, to fully grasp the broader implications of the Turkish data protection framework, it is necessary to delve deeper into the specific principles under the TDPL. By examining these principles in the context of AI, we can better appreciate the legal nuances and the essential balance required between advancing technology and safeguarding personal data.

2. THE GENERAL PRINCIPLES: NOT A HARBINGER OF INCOMPATIBILITY BUT AN ENABLER OF AI-DRIVEN PROCESSING

A key issue in the interplay between AI advancement and data privacy is the perceived tension between data protection regulations and the development of AI. The concern here centres on the notion that training, developing, or refining AI systems necessitates processing extensive datasets, which could potentially heighten privacy risks. While this data-intensive nature of AI systems might appear to conflict with general data protection principles, such as purpose limitation or data minimisation under both the GDPR and the TDPL, the reality is that data protection laws and the evolution of AI are not fundamentally at odds.

Data protection regulations, including the GDPR and the TDPL, are founded on principles that provide a degree of interpretative flexibility rather than imposing outright prohibitions on the processing of personal data for AI purposes or the generation of personal data by AI systems. These frameworks are designed to ensure that the handling of personal data, regardless of context, adheres to established privacy principles and regulations. The crucial factor is not merely the volume of data processed, or the methods employed but whether the processing activities comply with the legal requirements and principles set out in the respective data protection regimes. The flexibility of these principles is not a flaw in terms of legal certainty but rather a feature that allows these frameworks to be applied even as data processing practices evolve significantly.

More specifically, the TDPL enumerates the following general principles under Article 4:

- **Lawfulness and fairness:** This principle mandates that processing must be both lawful and fair, not only in general terms but also in accordance with applicable laws and secondary legislation[18]. It serves as an umbrella principle from which other principles, not

[18] For more information on this principle see Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, 2018); E. Eylem Aksoy Retornaz and Osman G. Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi' in E. Eylem Aksoy Retornaz and Osman G. Güçlütürk (eds), *Gelişen Teknolojiler ve Hukuk II: Yapay Zeka* (2021), p. 287; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 297; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 90;Elif Küzeci, *Kişisel Verilerin*

explicitly mentioned under the TDPL, can be derived and integrated into Turkish data protection law[19]. Both the Authority and legal scholars frequently invoke this principle to address areas not directly covered by the TDPL.

· **Accuracy and up-to-date maintenance:** Personal data processing activities must be based on accurate and up-to-date information, particularly when necessary. This principle does not require data controllers to ensure the accuracy of all personal data at every moment[20]. However, if circumstances arise that lead data controllers to suspect that the personal data they process may be inaccurate or outdated, they are obligated to verify the data's accuracy and currency by contacting the relevant individuals[21].

· **Specific, clear, and legitimate purposes:** Personal data must be processed for specific, clear, and legitimate purposes. This principle ensures that data processing is goal-oriented and transparent.

· **Relevance, limitation, and proportionality:** Data processing must be relevant, limited, and proportionate to the purposes for which the data is processed. This principle guards against the over-collection and misuse of personal data.

· **Storage limitation:** Personal data may only be stored for the duration specified by law or, if no such duration is specified, for the period necessary to fulfil the purpose for which the data is being processed.

The most challenging ones among these principles for the purposes of aligning AI with the TDPL are the principles of purpose being clear as well as limited, limiting the access of AI developers to readily available personal data collected for other purposes. Hence, these two principles, along with the data minimisation principle, which is not explicitly mentioned under Article 4, shall be explored in detail.

2.1. a. Processing for specific, clear and legitimate purposes

According to Article 4(2)(c) of the TDPL, personal data can only be processed for specific, explicit, and legitimate purposes. The requirement for specificity involves not only articulating the

Korunması (4 edn, On İki Levha Yayıncılık 2020), p. 228; Naciye Yücedağ, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler' (2019) 1 Kişisel Verileri Koruma Dergisi 47, p. 48.

[19] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, p. 2; Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 287; Küzeci, *Kişisel Verilerin Korunması*, p. 228; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 298;

[20] Küzeci, *Kişisel Verilerin Korunması*, p. 244; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 299.

[21] Fore more information on this principle see Küzeci, *Kişisel Verilerin Korunması*, p. 244; Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku* (2 edn, On İki Levha Yayıncılık 2019), p. 62; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 299; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 101; Yücedağ, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler', p. 50.

purposes in a clear and precise manner without using overly broad terms but also ensuring that potential uses not selected as purposes are excluded[22]. The purposes for processing personal data must be understandable and identifiable not only by the data controller or processor but also by the data subjects[23]. For instance, the Board has concluded in one of its decisions that a data controller providing transportation services through a mobile application violated both the principles of lawful and fair processing and the principles of processing for specific, clear, and legitimate purposes by using collected customer data for customer scoring without mentioning it in the privacy notice or terms of service[24].

The purpose for processing personal data must also be legitimate. According to the Board, legitimacy means that the purpose of the processing should be connected to and necessary for the activities of the data controller[25]. However, since legitimacy is a broad term open to interpretation, caution is necessary when assessing it. For example, guidance from the Board stipulates that processing customers' maiden names by a ready-to-wear clothing store for the purpose of selling clothes would not be a legitimate purpose[26]. This example initially discusses the storage of data unsuitable for the purpose rather than an illegitimate purpose per se. Additionally, even in this scenario, further analysis of the purpose is required. Given the personal nature of a maiden name, which is often used as a security question for verification purposes, it may be considered legitimate for ready-to-wear stores to process mothers' maiden names for security purposes, provided that customers are adequately informed.

In the GDPR, legitimacy is not explicitly defined but is generally described in relation to the purpose in Recital 39. From this, it can be inferred that legitimacy is connected to the principle of proportionality, indicating that the purposes should not disproportionately affect the rights and freedoms of the individuals concerned in favour of the interests of the data controller. This emphasises the need for a balance between the data controller's objectives and the fundamental rights and liberties of the data subjects, ensuring that data processing does not excessively infringe upon the latter.

In the context of processing personal data to train AI models, if individuals are only informed that their data will be processed "for the purpose of developing an AI model," such a purpose cannot be considered specific or clear, especially regarding the training of advanced models[27]. This is because advanced AI models vary in both design and functionality and may be intended to produce outputs within a specific domain or to undertake more general tasks, as seen with LLMs. Merely

[22] See Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, p. 7; Küzeci, *Kişisel Verilerin Korunması*, p. 30; Yücedağ, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler', p. 52; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 300.
[23] Yücedağ, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler', p. 53; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 301.
[24] Turkish Data Protection Decision No. 2020/65.
[25] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, p. 7.
[26] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, p. 8.
[27] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 301.

referencing the tool or method being used while concealing the true objective will not suffice to say that the purpose is specific or clear, and processing data without clearly informing the data subject of the specific purpose would certainly violate this principle[28].

For example, in cases where financial institutions process personal data to develop and generate outputs using an AI model for credit rating applications, the purpose should be articulated as "calculating creditworthiness and credit scores using machine learning algorithms to determine whether to lend credit to customers." This purpose directly explains the reason for processing the personal data as well as the potential implications, which are closely intertwined with the processing purpose. However, when determining whether the purpose is specific, potential additional purposes must also be considered. For instance, if the financial institution processes personal data not only to calculate the individual's creditworthiness and score but also to improve the model's accuracy and efficiency, the purpose must be explicitly stated as "calculating creditworthiness and credit scores using machine learning algorithms to determine whether to lend credit to customers and improving the model to produce more accurate results" to ensure the purpose is considered specific[29].

Even with this level of detail, questions may still arise about whether these purposes are sufficiently specific or clear since, despite the technical complexity of AI systems or models, no information is provided about the technical steps involved in processing the data[30]. Advanced AI systems and models indeed rely on highly complex mathematical processes. However, clarifying the purpose does not require providing individuals with detailed information about every stage of processing related to that purpose[31]. It is important to note that having a clear or specific purpose does not always require specifying the method by which personal data will be processed. For example, when processing address and phone information to deliver a product purchased from an online shopping site, it is sufficient to state the purpose as "delivering the product to the purchaser within the scope of an online sales contract and maintaining communication with the purchaser during this process[32]." However, if the method used for processing personal data significantly affects the purpose and outcome of the data processing, the method should be identified in a way that does not create a misleading impression on the data subject for the purpose to be considered specific and clear[33]. Although it is difficult to establish a definitive test here, as a rule of thumb, if the individual's opinion or reaction to the processing of their personal data would likely change if they were aware of the method, then the method of data processing should be included within the purpose to be considered clear to the individual. Considering examples where AI models have engaged in discriminatory hiring practices, it is likely that a prospective employee would react differently to the purpose of "evaluating job candidates and concluding the hiring process"

[28] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 301.
[29] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 302.
[30] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 302.
[31] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 302.
[32] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 302.
[33] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 302.

compared to "evaluating job candidates and concluding the hiring process using artificial intelligence[34]." Even if data subjects cannot influence the processing method, given the availability of remedies they may pursue depending on the nature or implications of the AI-driven processing of their personal data, the techniques, algorithms, or even more specific technical details that would affect such implications must be disclosed for the purpose to be considered specific or clear[35].

Whether a given purpose is legitimate must also be determined after careful consideration. Legality is required but not sufficient for legitimacy. If the purpose of the processing is illegal, it will violate this principle, possibly in addition to the principle of "lawfulness and fairness". One may question here what distinguishes these two principles. There are two main differences[36]: First, the principle requiring that the purpose of processing must be legitimate specifically targets the purpose rather than the processing itself, whereas the principle of lawfulness and fairness targets the whole processing activity. Secondly, legitimacy is a broader concept than legality, and legal actions may still be considered illegitimate. For instance, processing personal data to create fake news that influences people's political views would violate the principle that processing must be for legitimate purposes since such a processing purpose is not legitimate, even if the legality of such an action remains in a grey area under Turkish law. Moreover, if this involves processing copyrighted works of a literary or scientific nature without the author's permission or any other licence, it would further violate the principle of lawfulness due to infringement of copyright law[37].

2.2. b. Keeping processing relevant, limited, and proportionate to the purpose

The second purpose-related principle—commonly referred to as the purpose limitation principle—stipulates that personal data collected for specific purposes can only be processed in ways that are related, limited, and proportionate to those purposes. This principle is crucial for ensuring that individuals maintain a certain level of control over the processing of their personal data[38].

The requirement of relevance to the purpose means that the personal data processing activity must be suitable for achieving the stated purpose. For example, processing the residence address and phone number of a purchaser to deliver a product bought from an online shopping site is related to the purpose, but processing data such as social security numbers, license plate numbers, or blood types is typically not related unless there are special circumstances[39].

Taking this further, the proportionality of the processing must be evaluated in light of the specific circumstances. Advanced AI models, particularly general-purpose ones, are often developed to

[34] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 303
[35] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 303.
[36] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 303.
[37] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 303.
[38] Hüseyin Murat Develioğlu, *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku* (2017), p. 46; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 303.
[39] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 304.

perform tasks that could otherwise be carried out by humans. Developing an AI model typically requires large volumes of data. This raises the question of whether processing large amounts of personal data to train an AI model is proportionate to the purpose when the same task could be accomplished by a human or by traditional, non-AI-based software with much less personal data processing. The availability of methods that process lesser amounts of personal data does not necessarily render the processing of personal data for developing a machine learning model disproportionate[40]. Two key points must be considered here.

First, it is important to distinguish between the processing of personal data during model training and the processing of that data to generate outputs from a pre-trained model[41]. The stage that requires processing large volumes of personal data is the model training phase, where the purpose is to train a machine learning model that will generate a specific type of output. Given the current state of AI technology, achieving this purpose without processing large volumes of personal data seems impossible without compromising the model's accuracy or efficiency.

Second, the proportionality assessment should not be limited to the amount of data processed but should also consider the effectiveness of the data processing, its suitability for achieving the purpose, and its ability to produce accurate and efficient results[42]. AI models can surpass human capabilities significantly in terms of speed and accuracy in certain tasks for which they are designed. The ability to achieve much faster and more accurate results could justify the processing of more personal data as a proportionate processing activity. However, the practice of the Board is helpful in this context to maintain the balance here. For instance, in one decision, the Board found that even if explicit consent had been obtained, processing users' credit history and financial information on an online shopping site violated the principle of purpose limitation on the ground that the processing of this information must be foreseeable by the data subjects[43]. Hence, processing information that is seemingly irrelevant or remotely relevant to the purpose of the processing solely in order to increase the efficiency of an output of an AI model may be interpreted as infringing this principle.

The third qualitative requirement within this principle is actual purpose limitation. Within the scope of the purpose limitation principle, how data may be processed for specific purposes must be considered alongside the data controller's obligation to provide information to the data subject as per Article 10 of the TDPL[44]. In other words, compliance with the purpose limitation principle will be assessed based on the purposes communicated by the data controller. If previously defined and communicated purposes are expanded or new ones are added, the data controller must fulfil the obligation to inform data subjects about these new purposes to avoid violating the purpose

[40] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p 305.
[41] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 305.
[42] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 305.
[43] Turkish Data Protection Board Decision No. 2020/173.
[44] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 301.

limitation principle[45]. For example, using an e-mail address collected in a CV for a specific position to send promotional e-mails about products and services would violate this principle[46]. While there are no rigid requirements for compliance with this principle, each processing activity should be individually assessed to determine whether it is indeed relevant, limited, and proportional to the purpose.

Under the GDPR, it is accepted that personal data can be processed for subsequent compatible purposes. As per Article 6(4) of the GDPR, if there is a valid lawful ground, personal data may be processed for purposes that are compatible with the original collection purpose. Recital 50 supports this by stating: "*The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required*."

However, the TDPL adopts a different approach from the GDPR. Under the TDPL, there is no explicit provision concerning processing for subsequent purposes, whether compatible or not. The preamble of the TDPL, however, states that the conditions for processing personal data must be met again if the data are to be processed for needs that may emerge later[47]. The relevant preamble states:

> "*In order for personal data to be processed to meet needs that may arise subsequently, the conditions for processing personal data must be separately fulfilled*.[48]"

The Board also emphasised a decision as follows

> "*... the performance of a new data processing activity for a purpose different from the one that justified the initial processing of the personal data must be based on at least one of the conditions listed in Article 5 of the Law, and it must independently comply with all the principles required for the processing of personal data as listed in Article 4 of the Law[49]*."

Furthermore, guidelines provided by the Authority make it clear that data controllers will be held accountable if they process data for purposes other than those initially communicated to the data subjects[50]. Based on the wording of the TDPL, its preamble, and the Board's guidelines, it must be concluded that data controllers cannot process personal data for subsequent purposes under the TDPL, even if those purposes are compatible with the original ones.

---

[45] See Turkish Data Protection Board Decision No 2019/78.
[46] See Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 293.
[47] See Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 122.
[48] See, Premble of Article 4 of the TDPL.
[49] Turkish Data Protection Board Decision No 2019/78
[50] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, 2018), p. 47.

This strict stance of the TDPL on subsequent purposes has been criticised in the literature as a shortcoming and an overly rigid approach[51]. We agree that requiring the conducting of all compliance procedures for any subsequent purpose without examining the connection and compatibility with the initial purpose may not be ideal due to practical reasons. However, the protection of personal data is a fundamental right safeguarded by the Constitution, and allowing changes in purpose could restrict this right from the perspective of the data subjects. Under Turkish law, limitations or restrictions on rights must be narrowly construed. Hence, an interpretation allowing for the processing of personal data for subsequent purposes that are compatible with the initial purpose, similar to the GDPR, without going through the entire procedure again, seems unlikely.

2.3. c. Data Minimisation

Another dimension of the purpose limitation principle is that the amount of personal data processed should be limited to what is necessary for the purposes for which it is processed. This principle, known as data minimisation, is rooted in the idea that no more personal data than is necessary for fulfilling the purpose should be processed[52]. For example, if a data controller operating an e-commerce website collects information about a customer's blood type or health conditions under the pretext of facilitating online shopping activities or enhancing the user experience, this would constitute a violation of the data minimisation principle[53].

Although the TDPL does not explicitly mention data minimisation, the principle is inferred from the broader principle of processing data in a manner that is purpose-limited and proportionate, as well as from the principle of lawfulness and fairness. Indeed, the Board has enforced this principle in its decisions. In one case, the Board issued an administrative penalty against a data controller for transferring more data than was requested by a court, citing a breach of the data minimisation principle and basing its decision on the principle of purpose limitation[54]. In another decision, the Board held that a data controller operating a gym violated the principle of "minimising the amount of data requested" by processing members' biometric data for gym entry[55].

It is important to note that data minimisation does not strictly mean that no new personal data can ever be processed for an already achievable purpose. The processing of new personal data is permissible as long as it is proportionate and related to the processing purpose, does not violate

[51] See Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 295; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 307; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, p. 69

[52] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 304; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 124.

[53] Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 295.

[54] See https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-.

[55] Turkish Data Protection Board Decision No. 2020/167. Also see Turkish Data Protection Board Decision No. 2020/915 and Turkish Data Protection Board Decision No. 2022/797.

the data minimisation principle, and provided that other requirements are met. Proportionality in this context refers to weighing the risks posed to the data subjects by processing the new personal data against the impact of such processing on achieving the intended purpose[56].

The most important question about the data minimisation principle is whether it prohibits all AI-driven processing where less data-intensive or even manual methods could accomplish the intended task. For example, CV review and monitoring are tasks that were traditionally performed by humans until quite recently. Does the fact that these tasks can be conducted by humans without intensive personal data processing mean that using more data-intensive AI methods would violate the data minimisation principle? The answer should be no. The data minimisation principle does not impose a direct restriction on the means of processing. Rather, it is a principle to be applied holistically. The minimum amount of data to be processed must be determined by considering the specific circumstances, including but not limited to the nature, means, purpose, and grounds of processing. In the case of AI-powered CV review, the data minimisation principle alone will not render such a practice unlawful. However, such processing may be unlawful due to the lack of other essential elements of lawful personal data processing, such as failing to disclose a clear and explicit purpose[57].

2.4. d. Evaluation

Upon reflection, the stringent application of these principles may initially appear as a potential barrier to the development and operational dynamics of AI. However, these principles are not inherently antagonistic to the needs of AI-driven data processing. Instead, they offer flexibility for implementing tailored practices and making transparent disclosures when integrating AI without amounting to a prohibition or substantial restriction. On the contrary, the inherent flexibility within these principles provides a vital mechanism for adapting the provisions of the TDPL to contemporary forms of data processing facilitated by AI[58].

This adaptability is crucial for the responsible and trustworthy deployment of AI technologies. This analysis suggests that while current privacy-related requirements for AI extend beyond mere lawful data processing, the inherent flexibility of the TDPL could serve as a conduit for integrating these broader requirements directly into the legal framework. For instance, it could be argued that the principle of fairness inherently demands the incorporation of elements of responsible and trustworthy AI into the standard requirements for lawful data processing. This approach not only aligns with legal expectations but also enhances the ethical deployment of AI technologies,

[56] Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 296.
[57] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 305; Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 297.
[58] See Aksoy Retornaz and Güçlütürk, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi', p. 300.

ensuring they operate within a framework that respects both individual rights and technological progress.

3. PROBLEMS WITH THE APPLICATION OF THE TDPL TO AI-RELATED PERSONAL DATA PROCESSING ACTIVITIES

Having established that there is no inherent incompatibility between the TDPL and the processing of personal data for or by AI in terms of general principles, the next question to explore is how the TDPL applies to such processing.

In principle, the TDPL applies to the processing of personal data for or by AI as it ordinarily applies to other technologies due to the absence of specific provisions for AI-related processing. However, given the broad and sometimes vague language of certain principles and conditions, the ordinary application of the TDPL requires a certain degree of interpretation and case-by-case analysis when AI is involved.

More specifically, despite the lack of inherent incompatibility, there are practical challenges posed by the data-intensive nature of AI and the increased ability of AI systems to identify patterns and connections between different data points. These challenges can be grouped into three main categories:

- **Blurring the line between personal and non-personal data:** The enhanced pattern recognition and connection identification capabilities of AI systems, when combined with the broad identifiability component of personal data as referred to under both the TDPL and the GDPR, render the distinction between personal and non-personal data increasingly blurry. This blurring occurs to the extent that many pieces of information may be linked to others in a manner that enables the identification of a natural person, a data subject, for the purposes of the TDPL and the GDPR[59].

- **Unforeseeable implications of AI-related processing:** The potential unforeseeable implications and effects of AI-related processing on data subjects make it challenging to identify the appropriate ground for processing. When the chosen ground is explicit consent, ensuring that the consent obtained is indeed valid becomes difficult.

- **Challenges of unexplainable AI models:** The fact that most advanced AI systems are built on unexplainable AI models—where identifying how different parts of the input data influenced the output is often practically impossible—complicates the process of informing data subjects about the processing and properly exercising their rights, particularly the right to erasure.

[59] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 291.

It is important to note that these challenges are not exhaustive, and given the extremely dynamic nature of AI technologies and the rapid advancements in the field, more challenges may emerge over time, or some of these may be resolved without the need for intervention. This article focuses specifically on one of these challenges: the identification of lawful grounds and the examination of the validity of consent in cases where processing is based on the consent of the data subject.

4. LAWFUL GROUNDS FOR PROCESSING PERSONAL DATA BY OR FOR AI

Identifying the lawful ground for processing personal data is pivotal for ensuring that AI operates within the bounds of legal and ethical frameworks. In the context of AI, where data can be utilised in complex and often unforeseen ways, establishing a clear and lawful basis for data processing becomes even more critical.

Under the TDPL, the grounds for lawful processing are outlined in Articles 5 and 6 for non-sensitive and sensitive personal data, respectively. For non-sensitive personal data, Article 5 provides explicit consent as a lawful ground in its first paragraph and necessity-based grounds in the second. However, according to the Board's practice, data controllers must first determine whether any of the necessity-based grounds apply to their processing[60]. Consent may be used as a valid ground for lawful processing only when none of these necessity-based grounds are applicable.

This chapter will examine two key issues that may become more complicated when AI is involved: first, the identification of the lawful ground for processing personal data for AI systems, and second, the suitability of consent in this context. For each issue, the questions of whether personal data can be processed to train a model and whether personal data can be fed into a pre-trained system or model will be addressed separately.

4.1. The question of hierarchy between different lawful grounds under the TDPL

Although the wording of Article 5 and the enumeration of legal grounds may suggest that explicit consent is the primary basis for processing and that the other legal grounds are exceptions, all the legal grounds listed in the article are legally of equal significance, with no hierarchy between them. The Board's practice is particularly influential in determining the practical order of examination. The Board views the obtaining of explicit consent when one of the legal grounds listed in Article 5(2) of the TDPL is present as an abuse of rights, given the potential for the data subject to be misled or confused[61]. This is because explicit consent can be withdrawn at any time, while the grounds listed under Article 5(2) are not dependent on the data subject's consent. Therefore, when assessing the legal grounds, it is a practical necessity to first determine whether any of the grounds

[60] See Turkish Data Protection Board Decision No. 2020/529.
[61] See https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi.

specified in Article 5(2) of the TDPL apply; only if none of these grounds is applicable should the option of obtaining explicit consent be considered.

Moreover, in alignment with this practice, the processing of personal data for or by AI should first be examined to determine whether it can be based on one of the legal grounds in Article 5(2) of the TDPL, and only afterwards should its connection with explicit consent be analysed.

4.2. Can necessity-based grounds be used for AI-driven processing?

The grounds provided under Article 5(2) are primarily designed to address specific practical scenarios where obtaining consent would either be redundant or impractical. At first glance, it may look like these grounds are not applicable for processing personal data for or by AI in most cases. However, due to the broad wording used on these grounds, there may be instances where AI-related personal data processing could be based on one of these grounds. In this chapter, the availability of necessity-based grounds under Article 5(2) for AI-related personal data processing will be examined.

4.2.1. Personal data processing based on the explicit provision by a law

The first necessity-based ground for processing personal data is when such processing is explicitly stipulated by law. In Turkish law, various regulations across different statutes necessitate the processing of personal data. For example, Article 75 of the Turkish Labor Code No. 4857 requires employers to maintain a personnel file for each employee, which includes their personal information[62].

However, there is no general provision, rule, or principle in Turkish law that explicitly authorises the use of personal data for or by AI. This raises the question of whether existing legal frameworks for data processing also cover AI-related processing. This question should be determined on a case-by-case basis[63].

It is important to emphasise that the requirement for processing to be "explicitly" stipulated by law must be carefully considered. The term "explicitly" here is understood to mean that a broad or blanket authorisation, not specifying the data processing, cannot serve as a valid legal ground for processing personal data[64].

For AI-related personal data processing, real uncertainty arises when there is a provision requiring the processing of personal data without specifying the means by which the data controller should perform the processing. In general, the TDPL does not heavily intervene in how data controllers or processors handle data, with certain exceptions concerning the security measures to be taken

[62] See Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p, 164.
[63] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 311.
[64] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 311.

under Article 12. The question here is whether the absence of an explicit reference to AI as a means of processing could be interpreted as granting data controllers the freedom to choose whatever means they consider suitable. Data controllers do not have absolute liberty to choose the means of processing personal data. However, the lack of reference to AI as a potential means of processing should not be understood as an exclusion either. The means of processing must be chosen by taking multiple factors into account, including, but not limited to, the impact of the means on the general principles, as well as the efficiency and proportionality of the means with respect to the purpose of the processing.

For instance, in addition to the labour law provision referred to above, Article 419 of the Turkish Code of Obligations ("TCO") states that an employer may use personal data related to an employee only to the extent necessary for assessing the employee's suitability for the job or fulfilling contractual obligations. Based on this provision, an employer might process an employee's personal data for performance evaluations, which could potentially be conducted using an AI system developed from past data. However, the collection of personal data from each candidate for the purpose of developing such an AI model or system cannot be justified by this provision due to the cumulative consideration of two main reasons. First, AI-driven processing is not a mandatory means for such performance evaluations. Further, such processing may adversely and unjustly affect the performance evaluation for a given employee due to biases of AI systems that may be connected to non-performance-related metrics. Here, it must be mentioned that, indeed, there are increasingly more measures that may be implemented to increase the transparency of how AI models work or how such biases can be mitigated. Nevertheless, given that bias detection and mitigation techniques used for advanced models are still mostly experimental, relying on a provision enabling employers to process personal data to evaluate performance should not be interpreted as a blanket permission for employers to conduct such analysis using AI[65].

4.2.2. Necessity for the formation or performance of a contract

Another lawful ground for processing personal data without obtaining consent is when the processing of personal data relating to the parties to a contract is both necessary and directly related to the formation or performance of the contract. For example, processing the address of a buyer in an online shopping transaction to fulfil the contract can be based on this ground. This lawful ground cannot be broadly interpreted to allow the use of data obtained within the scope of all contracts for AI systems. The subject and purpose of the contract in question must be specifically considered and taken into account, and the processing of personal data by or for AI must be central to the contract[66].

[65] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 312.
[66] See Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 167; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 312; Develioğlu, *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*, p. 61.

To rely on this ground, the contract must be between the data controller and the data subject, and the personal data of a third party cannot be processed on this basis. For instance, if a user wishes to benefit from AI-powered smart assistant services, processing the user's data by these systems is directly related to the service's content and is necessary for its provision. The technical nature of these assistants requires the processing of personal data through AI for them to function. However, processing the personal data of job applicants using AI for managing a recruitment process is not a necessity, which is a task that has been undertaken manually or with help from non-AI software for years. Therefore, such data processing activities cannot be justified on this ground[67].

It may be questioned whether the inclusion of a dedicated clause governing personal data processing practices by or for AI within a contract would be sufficient to make this ground applicable. This question must be answered negatively. The connection between the performance of the contract and the data processing activity must be carefully examined, and the mere inclusion of a clause should not be sufficient to establish a direct link to rely on the contractual necessity to process personal data. Interpreting this ground otherwise would mean allowing it to be used for any personal data processing activity through a mere inclusion of a provision in a type of contract, expanding the scope of the application of this ground extremely. The ideal threshold question here, for AI-related purposes, is whether the processing for or by AI is indeed necessary for the performance of the core obligations of the contract. In other words, this ground should not be applicable when AI is not central to the contract but is introduced as part of a secondary obligation or merely as an arbitrary means. Indeed, it must also be noted that whether AI-related processing is central to a given contract must be examined on a case-by-case basis, taking the specific circumstances of each case into account[68].

4.2.3. The necessity for compliance with the data controller's legal obligations

Another ground for processing personal data is the necessity for the data controller to fulfil a legal obligation. An example of processing within this scope could be the handling of bank account numbers for paying employee salaries[69].

This ground might seem to overlap with the necessity arising from an explicit provision of the law or the necessity associated with the performance of a contract since respecting rights and obligations arising from a legally valid contract may be considered a question of compliance with legal obligations in a broader sense. Indeed, there may be overlapping scenarios. Nevertheless, there are instances where, even in the absence of an explicit legal obligation or contractual provisions to process data, such processing is necessary to meet another legal requirement. For example, businesses may need to process customer personal data to comply with secondary

[67] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 313; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 167.
[68] See Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 167; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 313.
[69] Preamble of Article 5 of the TDPL.

legislation and decisions issued by independent regulatory authorities, such as the Capital Markets Board, the Banking Regulation and Supervision Agency, or the Energy Market Regulatory Authority. Similarly, if legal obligations arise from court orders or directives from competent public authorities, this ground may be applicable to relevant data processing activities[70].

Another aspect to consider in relation to this principle is the broad duties of care provided by law for certain professionals. For instance, Article 369 of the Turkish Commercial Code (Law No. 6102) ("TCC") outlines the duty of care for members of the board of directors and other persons responsible for management in joint-stock companies. Given the success of AI systems in tasks with significant statistical demands, one might question whether these care obligations could be interpreted to require the use of available AI systems. Or, in the context of a credit agreement, could a bank be considered legally obligated to use AI systems to assess an individual's credit risk with the aim of reducing the amount of unpaid loans? Again, this question should be answered negatively[71].

For this ground to be applicable, there must be a legal obligation, and the data controller should not have the discretion to choose whether to comply with that obligation[72]. However, it must be emphasised that this ground does not give unlimited discretion regarding the means of processing while complying with a given obligation. Additional elements, such as potential risks and legal implications of the means and the needs and practices of each sector, must be considered. Regarding the question of whether banks are legally obligated to use AI systems, despite the fact that AI systems can increase efficiency and accuracy in certain tasks, the technical expertise and costs associated with developing AI systems, particularly at the business model level, and associated risks of exposing legally as well as commercially sensitive banking sector data to AI systems support the conclusion that such a broad obligation cannot be imposed. Nevertheless, considering the rapid development of AI systems, it is prudent to monitor these advancements and assess them on a case-by-case basis. For example, if a system that has sufficient protections in place and gained approval by both the regulatory authorities as well as the sector emerges at any point, using such a system may indeed be considered a requirement as per the duty of care[73].

4.2.4. Processing personal data made publicly available by the data subject

Another lawful ground for processing personal data under the TDPL is if the data has been made publicly available by the data subject. To understand this, it is crucial to clarify what is meant by "publicly available." For data to be considered publicly available, there must be an explicit

[70] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 313; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p 170.
[71] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 314.
[72] Develioğlu, *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*, p. 63; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 170; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 314.
[73] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 314.

intention from the data subject to make the data public[74]. Data that has been leaked without the data subject's consent or shared within a restricted group cannot be considered publicly available[75] and the data must be accessible by an indefinite number of people[76].

A critical point here is that the availability of this ground is purpose-dependent, meaning that making personal data publicly accessible does not grant third parties the right to process that data for any purpose. Third parties must process the data in a manner consistent with the purpose for which the data was made publicly available by the individual. In other words, making personal data publicly accessible is different from making it publicly available for the purposes of this ground. For example, phone numbers shared on platforms used for online listings cannot be used by third parties to send marketing messages simply because the data is publicly accessible[77]. Similarly, profile pictures uploaded publicly on Facebook by its users cannot be shared on other platforms or used to create deepfakes or train image-generation models[78].

The Board has emphasised this distinction in one of its decisions regarding public disclosure as follows:

> "*Even if the complainant's personal data is accessible from a website where the complainant had previously disclosed it, the company's use of this information was not aligned with the purpose of making it public on the website. The company's data processing activities were not aimed at utilising the complainant's professional expertise but rather for requesting an appointment related to the company's operations. Therefore, it was concluded that the data processing activity by the company could not be evaluated under Article 5(2)(d) of the Personal Data Protection Law No. 6698*[79]*."*

Here, it is important to address a subtle distinction between this legal basis and its (nearly) equivalent for sensitive data under the newly amended Article 6 of the TDPL. The amendment to Article 6 that introduces a similar ground for sensitive data explicitly requires that processing under the respective legal basis must align with the original purpose intended by the data subject. In contrast, Article 5, which governs non-sensitive data, lacks such an explicit reference, raising questions about whether this omission implies a different standard for processing non-sensitive data.

---

[74] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, p. 75.
[75] E. Eylem Aksoy Retornaz, *Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake)* (2021), p. 99; Küzeci, *Kişisel Verilerin Korunması*, p. 398; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 315.
[76] Naciye Yücedağ, 'Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri' (2017) 75 İÜHFM 765, p. 779.
[77] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 315.
[78] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 315.
[79] Turkish Data Protection Board Decision No. 2019/331.

One interpretation could be that this difference signifies a deliberate divergence between the two provisions, suggesting that alignment with the initial purpose is not a requirement for non-sensitive data. However, we argue that despite the absence of explicit language in Article 5, the necessity to consider the data subject's intent is not eliminated. This view is reinforced by the Board's consistent practice, which has upheld the consideration of intent even in the absence of an explicit reference under Article 5.

The use of publicly accessible data to train AI models might seem appealing for creating large datasets. However, two key considerations must be taken into account in such data processing activities. First, it must be carefully determined whether the data being processed is indeed public. Data that is made accessible through a paywall, shared within a limited group, or accessed by third parties without the explicit action of the data subject cannot be considered publicly available under Article 5(2)(d). Second, compliance with other general principles, such as limiting the use of disclosed data to the purpose for which it was disclosed, must be ensured[80].

4.2.5. Necessity for the Establishment or Exercise of a Legal Right

Another legal ground under the TDPL for processing personal data without obtaining consent is when such processing is necessary for the establishment or exercise of a legal right. For example, an employer submitting an employee's personal data to a court in a lawsuit filed by the employee falls within this scope, as it is necessary for the employer to exercise their right of defence[81].

The fact that there is currently no general obligation to use AI nor any legal right specifically related to AI raises the question of whether the use of AI could be considered necessary for the establishment or exercise of a legal right. This question becomes particularly relevant in situations where AI systems are employed to establish facts, and the establishment or exercise of a legal right depends on determining such facts[82].

This ground does not distinguish between the sources of the rights in question. But what happens if the parties create a contractual right through a contract that can only be exercised by processing certain personal data for or by AI? Some scholars argue that for this ground to be applicable, the processing must still be factually necessary, and a contractual "necessity" would not qualify[83]. Others argue that rights arising solely from contracts that are not explicitly mandated by law would not fall within the scope of this provision[84]. In such cases, the processing of personal data by AI would often be directly related to the performance of the contract, making it possible to rely on the legal basis outlined in Article 5(2)(c) of the TDPL, as previously explained.

[80] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 316.
[81] See Preamble of Article 5 of the TDPL.
[82] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 316.
[83] Küzeci, *Kişisel Verilerin Korunması*, p. 400.
[84] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 317.

4.2.6. Necessity for legitimate interests of the data controller

The last of the necessity-based grounds deserving special examination is provided under Article 5(2)(f), which allows personal data to be processed without consent when "*the processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject*." It is essential not to interpret this ground as a broad or blanket justification[85]. To determine when this ground is applicable, it is necessary to understand what is meant by "legitimate interests" and how to balance these interests with the fundamental rights and freedoms of the data subject.

The Authority's guidelines on legitimate interests stipulate that the "*legitimate interest of the data controller pertains to the benefit and advantage that will be gained from the processing activity. The benefit obtained by the data controller should be legitimate and significant enough to compete with the fundamental rights and freedoms of the data subject, specific and present. It should be related to the ongoing activities of the data controller and should result in a benefit in the near future*[86]."

Here, the Authority has emphasised that the interest must not only be legitimate but also specific and present. However, these attributes are somewhat vague and may not be very helpful in determining what constitutes a legitimate interest under this provision. Additionally, the requirement for the interest to be "present" suggests that data processing based on an anticipated benefit may not be justified under this legal ground. It has been argued that the requirement for the interest to be "present" should be interpreted as the benefit being certain to arise from the processing rather than speculative and that the reference to "a benefit in the near future" within the same paragraph supports this interpretation[87].

In one of its decisions on legitimate interests, the Board emphasised several points that data controllers should consider when relying on this ground[88]:

1. *The benefit obtained from processing personal data must be comparable to the fundamental rights and freedoms of the data subject.*

2. *The necessity of processing personal data to achieve the stated interest.*

3. *The legitimate interest must be present, specific, and clear.*

[85] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, p. 79; Küzeci, *Kişisel Verilerin Korunması*, p. 402; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 317.
[86] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, p. 78.
[87] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 318.
[88] Turkish Data Protection Board Decision No. 2019/78.

4. There must be a benefit in achieving the interest that could not be achieved by other means without processing personal data.

5. When determining whether an interest is legitimate, transparent and accountability-based criteria must be considered, such as whether there is an impact on a large number of people and whether the interest is exclusively profit-related.

6. The data subject's fundamental rights and freedoms must be protected from foreseeable, clear, and imminent dangers.

7. Technical and administrative measures must be in place to ensure lawful processing and to prevent harm and violations.

8. Compliance with general principles in the processing of personal data must be ensured, and a balancing test must be conducted to compare the data subject's fundamental rights and freedoms with the data controller's legitimate interest.

After establishing these criteria, the Board ruled that a fuel distribution company could process license plate and product type information of consumer vehicles within the framework of its Vehicle Identification Project based on legitimate interest. This decision is significant as it indicates that the necessity criterion is not interpreted too strictly by the Board[89]. The data controller claimed that using the consumer's license plate was necessary for the improved performance of the sales contract during fuel sales and for ensuring the correct type of fuel was provided. It is important to note that this reasoning aligns more closely with the legal ground found under Article 5(2)(c) of the TDPL regarding the necessity of processing personal data directly related to the formation or performance of a contract. In normal circumstances, when a situation is deemed necessary for contract performance, relying on the more challenging ground of legitimate interest may not be the most prudent choice for the data controller[90].

Additionally, in this case, whether processing the license plate through a Vehicle Identification System was truly necessary for fulfilling the fuel sales contract is debatable. While implementing an automated system to match the vehicle's license plate with the fuel type used may speed up the process and reduce errors, it is not essential for preventing sales of the incorrect fuel type. Alternative measures, such as employee training or confirming the fuel type with the driver during refuelling, could also reduce such errors. Here, the data controller's choice to rely on Article 5(2)(f) instead of Article 5(2)(c) suggests that they recognised that the system was not strictly necessary for contract performance and found the balance test more favourable to their situation[91].

[89] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 320.
[90] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, pp. 320-321.
[91] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 320.

The Board's decision to allow reliance on TDPL Article 5(2)(f) in this case shows that the necessity criterion is not interpreted rigidly and that the possibility of achieving the same goal through other means does not automatically disqualify the necessity criterion. This is significant for processing personal data for or by AI, as it suggests that Article 5(2)(f) could be a valid legal ground, even when there is no strict necessity for using AI.

The next question becomes whether AI-driven personal data processing could be based on Article 5(2)(f). It is evident that data controllers may have an interest in using machine learning to process personal data. These interests may be extremely diverse, including making accurate investment decisions, hiring more efficient candidates, granting loans to individuals with a high likelihood of repayment, or providing a better user experience to customers, all of which can be efficiently achieved by AI. However, can these interests be considered legitimate interests? The concept of a legitimate interest is broad and ambiguous, necessitating a case-by-case assessment. Several issues must be considered when basing a specific data processing activity on Article 5(2)(f). The first is the legality of the processing. The processing must be lawful to be considered based on a legitimate interest. However, the legality is not sufficient alone for relying on the legitimate interest ground. Conversely, if an interest or the processing itself is unlawful, it cannot be based on the legitimate interest ground[92].

Moreover, a substantial balancing test must be conducted to evaluate both the data controller's interest in AI-related processing and the potential implications of such processing on data subjects. Accordingly, when evaluating the balance between the data controller's legitimate interests and the fundamental rights and freedoms of the data subject, a distinction must be made. When personal data are used as part of a training set in the development of AI models, the personal data will not be directly accessible within the model. Being merely statistical entries in large datasets, they do not significantly affect the outcomes concerning the data subjects whose data are processed. Thus, such usage should not be considered to significantly impact the fundamental rights and freedoms of the data subjects[93].

While an individual data subject's personal data may not significantly influence the outputs of a model, the aggregated personal data could potentially impact the group of individuals to which the model is applied. However, this impact cannot be directly considered as affecting the data subjects whose data are processed in the first place. In most cases where personal data are used as part of a training set for the development of AI models, the data controller's legitimate interests will outweigh the fundamental rights and freedoms of the individuals involved[94].

Another distinction must be made regarding scenarios where AI models or systems produce undesired outputs due to the general quality or characteristics of the dataset. For instance, the

[92] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 321.
[93] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 321. Also see Science Panel for the Future of and Technology, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020), p. 50.
[94] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 322.

distribution or representation of the gender or race of employees or job applicants whose personal data are used to train a model intended for employment decisions may cause the model to discriminate. Processing personal data to train AI systems or models that could potentially produce unlawful outcomes can still be based on this ground, provided that the unlawfulness of the outputs cannot be directly linked to the processing or foreseen with a reasonable level of assurance. However, running the discriminatory model or system after becoming aware of the discrimination would be unlawful, and feeding any personal data to such a system or model would constitute unlawful processing, prohibited by the general principles explained above.

The situation changes further when personal data are fed as input or prompts into AI models. When an AI system processes personal data, it could generate outputs containing sensitive information, such as names, credit risk, job performance, health status, and sexual orientation, or outputs affecting individuals directly, such as denying them a job or access to financial or medical services. The misuse of this data for different purposes may also cause significant harm to the data subjects involved. Therefore, in such cases, it is particularly crucial that the purposes for using the outputs produced by providing personal data as inputs for AI models and the security measures taken by the data controller to prevent third-party access to this data be thoroughly reviewed before assessing the impact on the data subject's fundamental rights and freedoms.

Regarding the necessity element for data processing, it must be noted that processing by or for AI alone does not constitute a necessity per se. Nevertheless, one could argue that involving AI in personal data processing may assist in achieving quicker and more accurate results, thereby fulfilling the necessity criterion, at least in a practical sense. However, from the TDPL's perspective, we believe that the potential to generate new personal data through AI and the risk of this data being misused to harm individuals might prevent the Board from broadly interpreting the necessity criterion for data processing by or for AI. While interpreting the necessity criterion in a way that justifies the processing of personal data for or by AI on the basis that it is more effective than other available tools or means aligns with the realities of the digital era, such an interpretation may be constrained by the general principle of Turkish law that interpretations of fundamental rights and principles must be narrow[95].

In light of the above, despite our view that legitimate interest may be available for a broader range of AI-related personal data processing activities, it is safer to conclude that, in many cases, AI-related processing may not be based on a necessity-based ground as per Article 5(2). Consequently, explicit consent will often be relied on as the legal ground for such processing.

4.3. Can consent be used for AI-related personal data processing?

To begin with, the lawful ground for personal data processing under Article 5(1) of the TDPL requires not just any consent but explicit consent, which is defined as "freely given, specific, and

[95] See Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 322.

informed consent" under Article 3(1) of the TDPL. Keeping that in mind, in this chapter, we will use the term "consent" without repeatedly emphasising its explicit nature for the sake of simplicity.

What constitutes valid consent under Article 5(1)? First, despite the common practice of obtaining written statements primarily for evidentiary purposes, a written statement is not required for valid consent. What is required is a positive action, of which a written statement is just one form. For instance, consent is typically obtained by ticking a box on websites where data is primarily collected for developing or improving AI models, and this action is considered a valid positive step on the part of the data subject[96].

Furthermore, considering the legal definition, valid consent can be broken down into three fundamental components: (1) it must be specific to a certain subject; (2) it must be based on informed understanding; and (3) it must be expressed through free will. However, the technical functioning of modern AI raises several questions concerning all these elements since AI systems frequently process data in ways that may not have been fully anticipated at the time the data was collected. This could potentially render the original consent invalid due to a lack of specificity and informed understanding by the data subjects[97].

The requirement that explicit consent must be specific to a given issue implies that the data subject's consent must be clear, and general or open-ended consent is not valid[98]. This requirement is closely linked to the principle of purpose limitation, as the purpose must also be specific and limited. Often, whether the consent is specific will be determined according to the purpose of data processing. New purposes that extend beyond those initially determined by the data controller and included in the individual's consent require obtaining new consent.

The necessity of free will demands that data subjects act with conscious awareness when consenting to the processing of their personal data[99]. Factors that may impair an individual's will likewise affect the validity of their consent. In this context, it is important to examine how imbalances in knowledge and power between the parties influence the validity of such consent. If refusal to consent to data processing results in adverse consequences for the individual or inhibits access to a product or service, the consent cannot be deemed to have been freely given[100].

Furthermore, the validity of consent for personal data processing by or for AI must be evaluated, considering the nature of the AI in question. If personal data processing for or by AI is based on consent, it is imperative that data subjects are comprehensively informed about how their data will be processed and that they give their consent knowingly and voluntarily. This raises the question

[96] Kişisel Verileri Koruma Kurumu, *Açık Rıza Rehberi*, 2016), p. 3.
[97] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 323
[98] Kişisel Verileri Koruma Kurumu, *Açık Rıza Rehberi*, p. 4.
[99] Kişisel Verileri Koruma Kurumu, *Açık Rıza Rehberi*, p. 5.
[100] Kişisel Verileri Koruma Kurumu, *Açık Rıza Rehberi*, p. 6. Also see Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 324; Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku*, p. 160.

of whether the so-called "black box" nature of modern AI impacts this requirement. The intrinsic opacity of these AI systems may hinder the complete information of individuals regarding the processing of their personal data. However, data controllers or processors are not required to disclose the detailed technical methodologies of their precise data processing mechanisms[101].

Additionally, given the nature of AI, data initially collected for one purpose might be repurposed, and algorithms—whether intentionally or otherwise—may yield results that deviate from initial expectations. Such scenarios could potentially undermine the validity of the consent and may also violate the principle of purpose limitation[102].

These considerations highlight the challenges of ensuring the validity of consent given by data subjects for the processing of their personal data by or for AI. Furthermore, consent is the most commonly chosen ground for such processing in practice. This is not surprising due to the unsuitability of necessity-based grounds for AI-driven processing, as previously explained, but it is also problematic because this network of seemingly valid but essentially questionable consent creates the impression that data subjects are fully informed about the processing of their personal data by or for AI and have consented accordingly. Meanwhile, data controllers are often compelled to adhere to this practice to protect themselves for practical reasons.

In light of the complexities surrounding consent in AI-driven personal data processing, it becomes evident that while consent often serves as the primary legal basis, it carries significant challenges. These challenges include ensuring that consent is truly informed, specific, and freely given in an environment where AI's 'black box' nature can obscure the full understanding of data usage. Additionally, considering AI's continuous need for data, obtaining consent for every granular AI-related processing, as well as documenting it, may constitute a substantial practical burden.

CONCLUSION

In light of the explanations above, this article reaches three main conclusions regarding the intersection of AI and the TDPL. Firstly, the provisions of the TDPL are not inherently incompatible with the processing of personal data by or for AI. The core provisions of the TDPL, such as the general principles and lawful grounds for data processing, offer a degree of flexibility that allows for AI-related processing to occur in a manner that is compliant with the law. This adaptability within the TDPL demonstrates that, with careful application and interpretation, AI technologies can operate within the existing legal framework without undermining the protection of personal data.

Secondly, while the grounds provided under Article 5(2) may not initially appear directly relevant to AI-related processing due to their necessity-oriented nature, there is potential for their application in specific contexts. AI-driven data processing is often a choice rather than a necessity,

[101] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p, 325.
[102] Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, p. 325

which complicates the reliance on these grounds. However, the ground related to legitimate interests may be particularly useful for AI-based processing activities where no life-affecting decisions are made, offering a pathway for compliance in certain non-critical applications of AI.

Finally, despite being the most common ground for AI-related personal data processing, consent may not be the most practical choice. The inherent challenges associated with obtaining truly informed, specific, and freely given consent in the context of AI—due to its complex and often opaque nature—highlight significant practical and ethical concerns. The 'black box' nature of AI and the potential for data repurposing make it difficult to ensure that consent remains valid over time, thereby questioning its effectiveness as a legal basis for AI-related processing.

In conclusion, while the TDPL provides a flexible and adaptable framework for the lawful processing of personal data by or for AI, significant challenges remain, particularly in the practical application of consent and the necessity-based grounds. To address these challenges, ongoing dialogue and adaptive legal reasoning are essential. Legislators, regulators, and stakeholders must work together to refine existing frameworks and possibly develop new regulatory approaches that effectively address the unique demands of AI, ensuring that technological progress does not come at the expense of fundamental data privacy rights.

REFERENCES

1. Aksoy Retornaz EE, *Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake)* (2021)
2. Bayraktar K and others, *Özel Ceza Hukuku Cilt III: Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar* (On İki Levha Yayıncılık 2018)
3. Çekin MS, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku* (2 edn, On İki Levha Yayıncılık 2019)
4. Develioğlu HM, *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku* (2017)
5. Ekmekçi Ö and others, *Kişisel Verilerin Korunması Hukuku* (On İki Levha Yayıncılık 2024)
6. Güçlütürk OG, *Yapay Zeka ve Verinin Kullanımı* (2022)
7. Kişisel Verileri Koruma Kurumu, *Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence* (Kişisel Verileri Koruma Kurumu 2021)
8. Küzeci E, *Kişisel Verilerin Korunması* (4 edn, On İki Levha Yayıncılık 2020)
9. Oğuzman K, Seliçi Ö and Oktay-Özdemir S, *Kişiler Hukuku* (Filiz Kitabevi 2018)
10. Aksoy Retornaz EE and Güçlütürk OG, 'Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi' in Aksoy Retornaz EE and Güçlütürk OG (eds), *Gelişen Teknolojiler ve Hukuk II: Yapay Zeka* (2021)
11. Kim B and others, *Neural Networks Trained on Natural Scenes Exhibit Gestalt Closure* (2020)
12. Addy W and others, 'AI in credit scoring: A comprehensive review of models and predictive analytics' (2024) 18 118
13. Dellermann D and others, 'Hybrid Intelligence' (2019) 61 Business & Information Systems Engineering 637
14. Han X and others, 'Pre-trained models: Past, present and future' (2021) 2 AI Open 225
15. Kühl N and others, 'Human vs. supervised machine learning: Who learns patterns faster?' (2022) 76 Cognitive Systems Research 78
16. Yücedağ N, 'Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri' (2017) 75 İÜHFM 765
17. Yücedağ N, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler' (2019) 1 Kişisel Verileri Koruma Dergisi 47
18. Kişisel Verileri Koruma Kurumu, *Açık Rıza Rehberi*, 2016)
19. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, 2018)
20. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, 2018)
21. Kişisel Verileri Koruma Kurumu, *Sohbet Robotları (ChatGPT Örneği) Hakkında Bilgi Notu*, 2024)
22. Panel for the Future of S and Technology, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020)