

BİÇER GÜNER

Attorneys-at-Law

Bimonthly Data Protection and Privacy Bulletin

April 2024



Dear Readers,

As Biçer Güner Attorneys-at-Law, we are pleased to share with you our bi-monthly newsletter on the recent developments in the field of Personal Data Protection in Türkiye. In this newsletter, we will briefly inform you on the amendments to the Personal Data Protection Law No. 6698 and its effects, decisions of the Constitutional Court regarding the legislation and practice, the latest information note published by the Personal Data Protection Authority, and recent developments in our country and around the world.

Content

1. Amendments To The Personal Data Protection Law No. 6698	1
2. Information Note On The Personal Data Processing Requirement Stipulated In The Laws Has Been Published!	2
3. Constitutional Court Decision On The Violation Of The Right To Request Protection Of Personal Data Due To Failure To Conduct An Effective Criminal Investigation	3
4. Constitutional Court Decision On The Annulment Of Presidential Decree Provisions Within The Scope Of The Right To Demand Protection Of Personal Data.....	4
5. Latest News From Türkiye And The World!	4



1. Amendments to the Personal Data Protection Law No. 6698

Law No. 7499 on Amendments to the Code of Criminal Procedure and Certain Laws, which envisages long-awaited amendments to the Personal Data Protection Law No. 6698 ("**Law**"), was published in the Official Gazette dated March 12, 2024, and numbered 32487. The amendments, which aim to harmonize with the European Data Protection Regulation ("**GDPR**") and eliminate the long-standing problems regarding the processing of special categories of data, transfer of personal data abroad, administrative fines, and the appeal authority, will enter into force on June 1, 2024. The relevant amendments are briefly summarised below.

i. Special Categories of Personal Data

With the amendment to the Law, the conditions for the processing of special categories of personal data have been expanded and the distinction between data relating to health and sexual life and other special categories of personal data has been abolished in the conditions for the processing of special categories of personal data, and the legal grounds of the compliance with the law determined for the processing of special categories of personal data have been regulated to be valid for all special categories of personal data without any distinction. Within this scope, special categories of personal data may be processed with the explicit consent of the data subject or without the explicit consent of the data subject in cases prescribed by law, in cases of actual impossibility, publicization, in cases where it is mandatory for the establishment, exercise or protection of a right. Moreover, special categories of personal data can be processed without the explicit consent of the data subject, in case it is mandatory for the fulfilment of legal obligations in the field of employment, occupational health and safety, social security or social services and social assistance, and by foundations, associations or other non-profit organisations or formations established for political, philosophical, religious or trade union purposes, special categories of personal data belonging to their current and former members and members or persons who are

in regular contact with these organisations and formations, may be processed without the explicit consent of the person concerned provided that they comply with the legislation to which they are subject and their purposes are limited to their fields of activity and are not disclosed to third parties. These amendments aim to eliminate the problems experienced in practice while processing the special categories of personal data, such as the inability of Occupational Health and Safety experts to collect health data without explicit consent, the hesitations of lawyers while submitting the health data of employees who have left their jobs within the scope of the right to defense without the court's request, the issues emerged by sharing blood type and allergy information in an area accessible to everyone for use in emergencies, and the reliance on the explicit consent requirement in the processing of health data declared in CVs.

ii. Abroad Transfers

Prior to the amendment of the Law, in practice, the transfer of personal data abroad was mostly subject to obtaining the explicit consent of the data subjects, which resulted in certain difficulties, especially in commercial life. With the amendments introduced, it is envisaged to comply with both the requirements of the times and the regulations in the GDPR in terms of data transfer abroad. Accordingly, personal data may be transferred abroad without the explicit consent of the data subject in the presence of one of the following conditions:

- The presence of one of the legal reasons foreseen for the processing of personal data in Articles 5 and 6 of the Law and the "adequacy decision" to be made by the Personal Data Protection Board ("**Board**") specific to the country of transfer or the sector or international organization in the country of transfer.
- If personal data will be transferred to the country, a sector within the country, or an international organization where there is no adequacy decision, the presence of one of the "adequate safeguards" and the possibility of the data subject to exercise his/her rights and to apply for effective legal remedies in the country of transfer.
- If personal data will be transferred to the country, sector within the country, or international organization where there is no adequacy decision and if one of the "appropriate assurances" cannot be provided, exceptional transfers for single or discontinuous data transfers.
- Notification to the Board in case of the existence of Binding Corporate Rules ("**BCR**") approved by the Board or the standard contract to be prepared by the Board and one of the legal reasons specified in Articles 5 and 6 of the DP Law.
- In the absence of a BCR approved by the Board and a standard contract to be issued by the Board, obtaining permission from the Board for data transfer between group companies in the event that the companies have their own data transfer agreement.

It is worth noting that the onward transfers of data controllers currently located abroad to data controllers located in another country are also considered as abroad transfers in line with the Board's decisions.

With the amendments, it is expected to meet the needs arising from the dynamism of technology digitalization, and commercial life by paving the way for the lawful use of cloud-based software and applications, most of which are frequently used by companies and whose servers are located abroad. However, data transfers abroad should be regulated in more detail, and the guidelines and regulations to be prepared by the Board should be guided in practice.

iii. Other

Pursuant to the Amendment, the data controller or data processor is obliged to notify the Personal Data Protection Authority within 5 (five) business days following the signing of the standard contractual clauses described above. In the event that the notification obligation is not fulfilled, an administrative fine from TRY 50,000 to TRY 1,000,000, effective for the year 2024, will be imposed on the data controller or data processor. We would like to note the fact that this administrative fine can also be imposed on data processors is a first in the field of application of the Law.

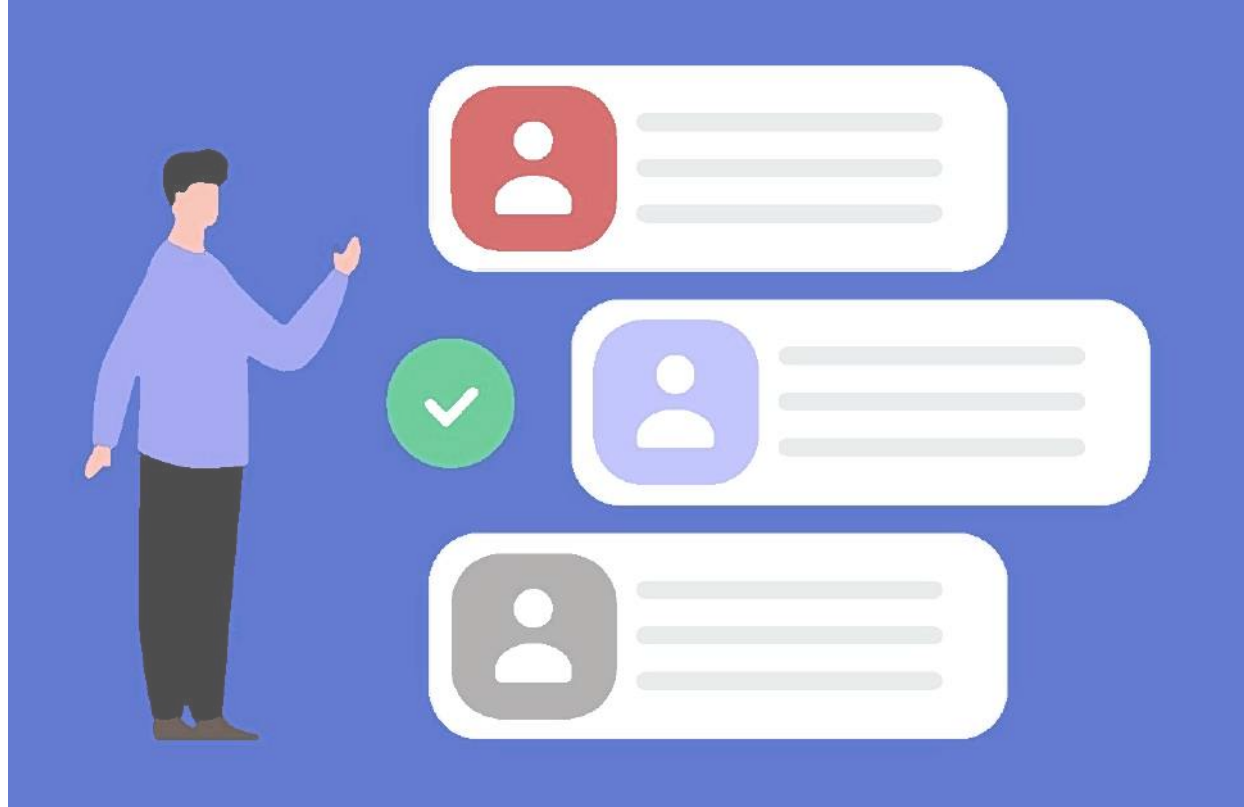
In addition, the procedure of filing a lawsuit before the administrative courts instead of applying to the Criminal Courts of Peace against the administrative sanction decisions issued by the Board has been envisaged. Pursuant to the transitional provision added to the Law, the files before the criminal judgeships of peace as of June 1, 2024, will be finalised by these judgeships. Finally, the existing provisions of the Law regarding transfers abroad will continue to be in force until September 1, 2024, together with the new provisions.



2. Information Note on the Personal Data Processing Requirement Stipulated in the Laws has been Published!

The Personal Data Protection Authority ("**Authority**") has published an Information Note on the Personal Data Processing Requirement Stipulated in the Laws ("**Information Note**") regarding the personal data processing requirement stipulated in Article 5/2-a of Law No. 6698 on the Protection of Personal Data, which is defined as "*explicitly stipulated in the laws*". The Information Note, published on the official website of the Authority on February 12, 2024, evaluates the requirement "*explicitly stipulated in the laws*," which enables the processing of personal data without the explicit consent of the data subject when it is clearly stipulated in the laws, within the scope of Turkish and European Union Law and provides examples of its implications in practice. Highlighted important assessments in the Information Note are briefly as follows:

- The protection of personal data has acquired the status of a fundamental right with the amendment made in 2010 under Article 20 of the Turkish Constitution. Accordingly, like all other fundamental rights and freedoms, the protection of personal data can be restricted only by law without infringing on the essence of the right in accordance with the principles in Article 13 of the Turkish Constitution. In this context, Article 28 of the Law, which regulates exceptional cases where the Law cannot be applied within the scope of the right to the protection of personal data, constitutes a limitation imposed by law on this right.
- As per the wording of the provision foreseeing that fundamental rights and freedoms can only be restricted by law, these rights and freedoms cannot be regulated or restricted by means such as regulations, directives, or decrees with the force of law. In this context, the Authority has stated that regulatory actions of the administration cannot directly restrict a fundamental right, in other words, a new restriction cannot be created beyond the limitation brought by a specific law in accordance with the Turkish Constitution. For example, in accordance with the principle of the indivisibility of legislative power, the regulation granting direct regulatory authority to the Information Technologies and Communication Authority regarding the processing of personal data and the protection of privacy was annulled by the Constitutional Court's decision numbered 2013/122 M., 2014/74 D.
- Additionally, the Authority emphasizes that regulations aimed at strengthening fundamental rights and enabling more effective use of rights cannot be considered as restrictions and therefore the administration can make regulations by concretising the legal limitations. Therefore, it is stated that regulatory actions duly enacted by the administration within the legal framework remain binding within the administrative organization and must be implemented unless annulled.
- Furthermore, the authority to interpret the requirement "*explicitly stipulated in the laws*" for personal data processing specified in Article 5 of the Law lies within the discretion of the administration, but it is emphasized that this discretion cannot restrict the fundamental rights and freedoms. Thus, the Authority has emphasized that interpreting the wording of the provision regarding the "*explicit*" requirement would be contrary to the spirit of the Law and that the processing requirement can only be applied in very limited cases. Accordingly, the processing of personal data will only be possible, if there is a clear provision regarding the processing of personal data in any law or if guidance is provided to secondary legislation through a clear provision.
- When examining the European Union legislation on the subject, it is observed that although the GDPR does not separately regulate the provisions "*clearly stipulated in the laws*" and "*fulfilment of a legal obligation*" unlike Turkish law, it serves a similar purpose in practice.



- Pursuant to Recital 41 of the GDPR, the general purpose of the data controller is considered to comply with a legal obligation that has a sufficiently clear basis in general legal rules or special laws. If this obligation can be identified by reference to a specific legal provision or by referring explicitly to advice, a decision of the authority, or a guide, it will be considered as a legal obligation requirement. Similarly, according to the "Legal Basis for Processing Personal Data Guidance Note" published by the Irish Data Protection Authority, the legal obligation processing requirement can be indicated by secondary legislation as well as primary legislative regulations.

3. Constitutional Court Decision on the Violation of the Right to Request Protection of Personal Data Due to Failure to Conduct an Effective Criminal Investigation

With the "Application of Furkan Çakır Decision" ("**Decision**") numbered 2020/36976 and dated February 13, 2024, published in the Official Gazette dated March 22, 2024 and numbered 32497, the Constitutional Court ("**CC**") ruled that the right to request protection of personal data was violated due to the failure to conduct an effective criminal investigation regarding the complaint made by the employee ("**Applicant**") due to the employer accessing the employee's bank transactions without the employee's knowledge and consent to avoid paying labor receivables after terminating the employment contract.

In the case subject to the Decision, the Applicant filed a criminal complaint with the Samsun Public Prosecutor's Office ("**Prosecutor's Office**") on October 9, 2020, by alleging that he was accused by the employer of acquiring unlawful profit by using the company's authority, and he has also alleged that, in the criminal complaint against him, the employer requested the examination of a bank transaction by specifying the bank name, amount, and date, and it would not be possible for

the employer to know these details without accessing his personal data. The Prosecutor's Office stated that obtaining personal data through sensory organs and disclosing it to others would not constitute the crime of obtaining personal data unlawfully, but if the conditions are met, it could be evaluated as an invasion of privacy if there is a violation of private life; thus, it decided not to prosecute on the grounds that the formal elements of the crime were not met. Moreover, it was stated that apart from the abstract allegation made by the Applicant, there was no other evidence found.

The Applicant stated in his complaint petition that he had requested the Prosecutor's Office to write a letter to the banks and to hear his witness and that he also requested the investigation file regarding the criminal complaint made against him by the employer to be examined, however, a decision of non-prosecution was made on the grounds that there was no evidence other than abstract statements, and he has appealed the said decision before the Samsun 1st Criminal Judgeship of Peace ("**Judgeship**"). The Judgeship decided definitively to reject the appeal on the grounds that there was no irregularity in the aforementioned decision. Thereupon, the Applicant made an individual application to the CC on the grounds that an effective criminal investigation was not conducted on his complaint that his personal data had been unlawfully seized.

Firstly, the CC stated that not only information revealing one's identity but also all data that directly or indirectly identify a person are considered as personal data, including bank and credit card transactions. It emphasized that according to Article 20 of the Turkish Constitution, everyone has the right to demand the protection of their personal data, which includes being informed about personal data concerning oneself, accessing them, requesting their correction or deletion, and learning whether they are used for their intended purposes. Therefore, it was emphasized that the state is obliged not only to refrain from arbitrarily interfering with the protection of an individual's personal data but also to prevent attacks by third parties, and it has positive obligations in this regard, including establishing an effective judicial system for the resolution of disputes. Based on these assessments, it was concluded that in the concrete case, the incorrect evaluation of the nature of the offense due to the decision made on the file without taking the Applicant's statement and collecting the evidence he claimed in the complaint letter, resulted in the failure to provide an effective legal mechanism for the Applicant to present his claims and evidence, and thus, the positive obligation regarding the procedure was not fulfilled. Therefore, the CC ruled that the right to demand the protection of personal data under Article 20 of the Turkish Constitution, which is guaranteed within the scope of the right to respect private life, was violated. In this regard, a copy of the Decision was sent to the Samsun Public Prosecutor's Office for a new investigation to be conducted to eliminate the consequences of the violation of the right to demand the protection of personal data under the right to respect for private life.

In conclusion, with the Decision, it was emphasized that the state is obliged to provide individuals with an effective legal mechanism to present their claims and evidence, and it is also responsible for preventing attacks by third parties on individuals' personal data.

4. Constitutional Court Decision on the Annulment of Presidential Decree Provisions within the Scope of the Right to Demand Protection of Personal Data

With its decision numbered 2018/118 M. and 2023/180 D. and dated October 26, 2023, published in the Official Gazette dated February 27, 2024, and numbered 32473 ("**Decision**"), the Constitutional Court ("**CC**") abolished various provisions of the Presidential Decree on the Organization of the Presidency ("**Decree**") within the scope of the right to demand protection of personal data guaranteed by Article 20 of the Turkish Constitution.

In the relevant Decree, the CC stated that the regulations introduced by the Presidential Decree should not be related to the fundamental rights, personal rights, and duties under the First and Second Sections of the Second Part of the Turkish Constitution, political rights and duties under the Fourth Section, and the issues that are foreseen to be regulated exclusively by law or explicitly regulated in the law. Accordingly, the Decree's various provisions were abolished on the grounds that it was not possible to regulate the right to protection of personal data, which is included in the Second Part of the Turkish Constitution titled 'Rights and Duties of the Individual'. The provisions annulled and the reasons for annulment are briefly summarized as follows:

- The phrase 'collecting information' in the provision '*Collecting information about senior executives in charge of the administration and management of the state, keeping their registry summaries and biographies*' set forth under Article 8, paragraph (f) of the Decree, which is listed among the duties of the General Directorate of Personnel and Principles, which is one of the units of the Presidential Administrative Affairs, was abolished. In its justification for the annulment, the CC emphasized that the data to be collected on the senior executives in charge of the administration and management of the state would consist of personal data such as registry information reflecting the professional and special situations of the individuals, their resumes to include their business and social life; and stated that this regulation on personal data falls within the prohibited area that cannot be regulated by Presidential Decree.
- The phrase "any kinds of information and documents" in the 3rd paragraph of Article 33 of the Decree stating that "*The Boards may request any kinds of information and documents related to their areas of duty from the relevant ministries and public institutions and organisations. Such requests shall be evaluated by the institutions and organisations with priority.*", which regulates the working principles and procedures of presidential policy boards, and the phrase "necessary information" in Article 36 stating that "*The Boards are authorized to request the necessary information related to their duties from all public institutions and organisations. All public institutions and organisations from which information is requested are obliged to provide such information.*", which regulates the obligation of presidential policy boards to collect information and keep secrets, were abolished. The CC stated in the justification that as personal data are included in the scope of the phrases "any kinds of information and documents" and "necessary information," the relevant provisions are within the scope of the prohibited area that cannot be regulated by the Presidential Decree.
- Article 378 within the thirteenth section of the Decree, which regulates the authority of the Ministry of Health to collect, process, and share information, was annulled due to containing provisions regarding the collection, processing, transfer, and establishment of an access system to personal data related to health services, and ensuring the security of the system, within the prohibited area that cannot be regulated by the Presidential Decree. In order to prevent the annulment decision from creating a legal gap, it was decided for the annulment to enter into force after 9 months.

Consequently, with the Decision, it was emphasized that the right to demand protection of personal data guaranteed by Article 20 of the Turkish Constitution is one of the fundamental rights included in the "Rights and Duties of Individuals" title of the Second Section of the Turkish Constitution, and therefore regulations within this right cannot be introduced by the Presidential Decree.

5. Latest News from Türkiye and the World!

i. Türkiye

- ⇒ In cooperation with the Digital Transformation Office of the Presidency of the Republic of Türkiye and the United Nations Development Programme (UNDP), the '[Data Governance Framework - Recommendation Report for Türkiye](#)' was published to establish a governance framework that will define data access, use and sharing in Türkiye. In addition to this study, it was also stated that within the scope of the preparations for the National Data Strategy, legislative studies on open government data, data localisation and national data dictionary, as well as a comprehensive needs analysis and recommendation report on artificial intelligence data governance needs are in progress. It was stated that the National Data Strategy, which will become the final draft after the contributions of all stakeholders and the process of receiving opinions, will be completed at the beginning of 2025.
- ⇒ The Competition Board issued an [interim injunction](#) in the investigation initiated against META Platforms, Inc. ("**META**") on suspicion of abusing its dominant position by linking Threads and Instagram applications. It was assessed that META's merging of the data of users who created Threads profiles based on their Instagram accounts, without providing users with the option of consent, would cause irreparable harm until the investigation is completed. META's text-based social media platform Threads will be closed in Turkey as of April 29 to comply with the Competition Board's injunction.





- ⇒ The Advertising Board, affiliated with the Ministry of Trade, has examined e-commerce sites under the "Digital Consumer Protection Project" and [imposed administrative fines, cessation, and correction measures](#) on 12 e-commerce platforms, including Amazon Turkey, for making it difficult for users to unsubscribe, sharing personal data with third parties, engaging in targeted advertising, and making commercial message consent mandatory. The Advertising Board also analysed various texts such as membership agreements, informing, explicit consent, and cookie policies of companies and stated that consumers' decision-making or choice-making will be negatively affected and consumers are not clearly informed, which is misleading and contrary to the principles of fair competition.

ii. World

- ⇒ The Information Commissioner's Office (ICO) has published new [data protection penalty guidelines](#) to increase transparency in how penalties are applied and calculated. The guideline sets out the legal framework that empowers the ICO to impose fines, provide approaches to identifying the economic assets of a business or organization, and the methodology used to calculate administrative fines.
- ⇒ The Artificial Intelligence Act (AI Act), which provides the world's first comprehensive framework to limit the risks of artificial intelligence globally, was [approved by the European Parliament](#) on March 13, 2024. After undergoing a legal linguistic review called "corrigendum," the text will come into force on the twentieth day following its publication in the Official Gazette of the European Union (EUR-Lex), subject to the official approval of the European Council.
- ⇒ The French Data Protection Authority (Commission nationale de l'informatique et des libertés - CNIL) has published the [2024 Personal Data Security Guide](#), focusing on how personal data should be processed, especially in areas such as artificial intelligence, mobile applications, cloud computing, and application programming interfaces (APIs).

Additionally, CNIL announced the initiation of a public consultation until May 31st to ensure that multi-factor authentication solutions comply with the General Data Protection Regulation.

- ⇒ The European Data Protection Supervisor ('EDPS'), an independent supervisory authority enabling European institutions to uphold privacy and data protection laws, has stated that the European Commission ('**Commission**') has [breached](#) a number of key data protection regulations in the GDPR with its use of Microsoft 365. In this context, it was stated that; what kind of personal data will be collected when using Microsoft 365 and for what purposes they will be used is not adequately shown in the contract concluded between the Commission and Microsoft, the provisions of the legislation are violated in the transfer of personal data, and in this context, it was decided to instruct the Commission to stop the transfer to countries that are not covered by the adequacy decision, effective from December 9, 2024.
- ⇒ The Council of the European Union and the European Parliament have reached [a provisional agreement](#) on a new law to facilitate the sharing and access to health data across the EU. The proposed regulation for the European Health Data Space (EHDS) aims to enhance individuals' access to and control over their personal electronic health data and enable the reuse of certain data for public interest, policy support, and scientific research purposes.
- ⇒ The German Ministry of Health announced that the [Health Data Use Act](#) came into effect on March 26th. The law aims to advance health research by granting pharmaceutical companies access to patients' health data for research purposes. Accordingly, the data provided to researchers will be anonymized, and administrative fines will be imposed in case of privacy breaches.
- ⇒ In the state of Florida, a law proposing one of the strictest social media regulations for children has been [formalized](#). The regulation, which will come into effect on January 1, 2025, aims to eliminate the harmful effects on the mental health of children who excessively use social media platforms and protect them from risks such as anxiety, depression, and other mental illnesses as a result. The scope of the regulation includes social media platforms that support endless scrolling, display reaction metrics such as likes, contain autoplay videos and have live streaming and instant notification features.



- ⇒ The United States ('US') Senate [approved](#) the bill paving the way for the transfer of TikTok, of which Beijing-based Bytedance is the main shareholder, and the ban if it is not transferred. The US House of Representatives, in its vote on March 13, adopted the bill titled 'Protecting Americans from Foreign Adversary Controlled Applications Act' by a large majority and sent it to the US Senate for approval. US President Joe Biden, on the other hand, stated that if the Senate approves, he will sign the law and put it into effect. If the bill, which paves the way for the banning of TikTok on the grounds that it poses a national security threat, is enacted, ByteDance, the main partner, will have to transfer the platform. Otherwise, it is envisaged that TikTok will be removed from the internet application stores in the USA for 5 months or completely.

Should you have any queries on the above, please contact us.

Contact

Burçak Kurt Biçer <i>Managing Partner</i> burcak.bicer@bicerguner.com	Uğurkan Şeber <i>Senior Associate</i> ugurkan.seber@bicerguner.com	İrem Efe <i>Associate</i> irem.efebicerguner.com
-------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------

BİÇER GÜNER

Attorneys-at-Law

Bimonthly Data Protection and Privacy Bulletin

Nisan 2024



Değerli Okuyucularımız,

Biçer Güner Avukatlık Ortaklığı olarak, Türkiye'deki Kişisel Verilerin Korunması alanında meydana gelen gelişmelere ilişkin olarak iki ayda bir yayınladığımız bültenimizi sizlerle paylaşmaktan memnuniyet duyuyoruz. Bu bültenimizde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki değişiklikler ve etkileri, Anayasa Mahkemesi'nin mevzuat ve uygulamaya ilişkin kararları, Kişisel Verileri Koruma Kurumu tarafından yayımlanan en son bilgi notu ve ülkemizde ve dünyada yaşanan güncel gelişmeler hakkında siz değerli okuyucularımızı kısaca bilgilendirecek içeriklere yer veriyoruz.

İçerik

1. **6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Getirilen Değişiklikler.... 1**
2. **Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu Yayımlandı!..... 2**
3. **Etkili Bir Ceza Soruşturması Yürütülmemesi Nedeniyle Kişisel Verilerin Korunmasını İsteme Hakkının İhlali Hakkında Anayasa Mahkemesi Kararı 3**
4. **Kişisel Verilerin Korunmasını İsteme Hakkı Kapsamında Cumhurbaşkanlığı Kararnamesi Hükümlerinin İptaline İlişkin Anayasa Mahkemesi Kararı..... 4**
5. **Türkiye Ve Dünya'dan Güncel Haberler! 4**



1. 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Getirilen Değişiklikler

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("**Kanun**") uzun zamandır beklenen değişiklikleri öngören 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, 12 Mart 2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanmıştır. Avrupa Veri Koruma Tüzüğü'ne ("**GDPR**") uyum sağlamayı hedefleyen, özel nitelikli kişisel verilerin işlenmesi, kişisel verilerin yurt dışına aktarılması, idari para cezaları ve itiraz merciine ilişkin uzun zamandır süregelen sorunların giderilmesini amaçlayan düzenlemeler 1 Haziran 2024 tarihinde yürürlüğe girecektir. İlgili değişiklikler aşağıda kısaca özetlenmiştir.

i. Özel Nitelikli Kişisel Veriler

Kanun değişikliği ile özel nitelikli kişisel verilerin işleme şartları genişletilerek, özel nitelikli kişisel verilerin işleme şartlarında sağlık ve cinsel hayata ilişkin veri ve diğer özel nitelikli kişisel veri ayrımı kaldırılmış, özel nitelikli verilerin işlenebilmesi için belirlenen hukuka uygunluk sebepleri herhangi bir ayırım yapılmaksızın tüm özel nitelikli kişisel veriler için geçerli olacak şekilde düzenlenmiştir. Bu kapsamda değişiklik ile özel nitelikli kişisel veriler, ilgili kişinin açık rızası dahilinde veya kanunlarda öngörülen haller, fiili imkânsızlık hali, alenileştirme, bir hakkın tesisi, kullanılması veya korunması için zorunlu olması durumlarında ilgili kişinin açık rızası olmaksızın işlenebilecektir. Ayrıca, istihdam, iş sağlığı ve güvenliği, sosyal güvenlik veya sosyal hizmetler ile sosyal yardım alanındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması halinde ve siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek veya diğer kar amacı gütmeyen kuruluş ya da oluşumlar tarafından, tabi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut ve eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere ait özel nitelikli kişisel veriler, ilgili kişinin açık rızası olmadan işlenebilecektir.

Söz konusu değişiklikler ile uygulamada özel nitelikli kişisel veri işlenmesi kapsamında yaşanan; örnek olarak İş Sağlığı ve Güvenliği uzmanlarının sağlık verisini açık rıza olmaksızın toplayamaması, avukatların savunma hakkı kapsamında işten ayrılan çalışanların sağlık verilerini mahkeme talep etmeden sunarken yaşadığı çekinceler, kan grubu ve alerji bilgilerinin acil durumlarda kullanılmak üzere herkesin erişebildiği bir alanda paylaşılmasının yarattığı sorunlar, CV'lerde beyan edilen sağlık verilerinin işlenmesinde açık rıza şartına dayanılması gibi problemlerin önüne geçilmesi amaçlanmıştır.

ii. Yurt Dışı Aktarımlar

Kanun değişikliği öncesinde kişisel verilerin yurt dışına aktarılması pratikte büyük ölçüde ilgili kişilerin açık rızalarının alınmasına bağlı hale gelmiş, özellikle ticari hayatta birtakım zorlukları beraberinde getirmiştir. Getirilen değişiklikler ile yurt dışına veri aktarımı bakımından hem çağın gerekliliklerine hem de GDPR'daki düzenlemelere uyum sağlanması öngörülmüştür. Buna göre, aşağıdaki hallerden birinin varlığı halinde ilgili kişinin açık rızası olmaksızın kişisel veriler yurt dışına aktarılabilir:

- Kanun'un 5 ve 6. maddelerinde kişisel veri işlenmesi için öngörülen hukuki sebeplerden birinin varlığı ve aktarım yapılan ülke veya aktarım yapılacak ülkedeki sektör ya da uluslararası kuruluş özelinde Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") vereceği "yeterlilik kararı"nın olması.
- Yeterlilik kararı bulunmayan ülke, ülke içindeki sektör veya uluslararası kuruluşa kişisel veri aktarımı yapılacaksa, aktarım yapılacak ülkede ilgili kişinin haklarını kullanma ve etkili kanun yollarına başvurma imkanının bulunması ve "uygun güvence"lerden birinin varlığı
- Yeterlilik kararı bulunmayan ülke, ülke içindeki sektör veya uluslararası kuruluşa kişisel veri aktarımı yapılacaksa ve "uygun güvence"lerden birinin sağlanamaması durumunda tek veya süreklilik arz etmeyen veri aktarımlarına yönelik olarak istisnai olarak yapılan aktarımlar.
- Kurul'un onayladığı Bağlayıcı Şirket Kurallarının ("**BŞK**") varlığı veya Kurul'un hazırlayacağı standart sözleşmenin ve Kanun'un madde 5 ve 6. maddelerinde belirtilen hukuki sebeplerden birinin mevcut olması halinde Kurul'a bildirim yapılması.
- Kurul'un onayladığı BŞK ve Kurul'un hazırladığı standart sözleşme yoksa; grup şirketleri arasındaki veri transferine ilişkin şirketlerin kendi veri transfer sözleşmesinin mevcudiyeti halinde Kurul'dan izin alınması.

Belirtmek gerekir ki, halihazırda yurt dışında bulunan veri sorumlularının, başka bir ülkede yer alan veri sorumlularına yapacakları ikincil aktarımlar da Kurul kararlarıyla paralel olarak yurt dışı aktarım olarak değerlendirilmektedir.

Söz konusu değişiklikler ile şirketler tarafından sıklıkla kullanılan ve sunucuları yurt dışında bulunan ve çoğu bulut tabanlı yazılım ve uygulamaların hukuka uygun olarak kullanılabilmesinin yolu açılarak teknoloji ve dijitalleşme ile ticari hayatın dinamikliğinin doğurduğu ihtiyaçların giderilmesi beklenmektedir. Ancak, yurt dışı veri aktarımlarının daha detaylı olarak düzenlenmesi, Kurul tarafından hazırlanacak rehber ve yönetmeliklerin uygulamada yol gösterici olması gerekmektedir.

iii. Diğer

Değişiklik ile yukarıda açıklanan standart sözleşmenin imzalamasından itibaren 5 (beş) iş günü içerisinde veri sorumlusu veya veri işleyen tarafından Kişisel Verileri Koruma Kurumu'na bildirim yükümlülüğü getirilmiştir. Bildirim yükümlülüğün yerine getirilmemesi halinde veri sorumlusu veya veri işleyenler hakkında, 2024 yılı için geçerli olmak üzere, 50.000 TL'den 1.000.000 TL'ye kadar idari para cezası uygulanması öngörülmüştür. Söz konusu idari para cezasının, veri işleyenler hakkında da uygulanabilmesinin Kanun'un uygulama alanında bir ilk olduğunu siz değerli okuyucularımızla paylaşmak isteriz.

Ayrıca Kurul tarafından verilen idari yaptırım kararlarına karşı sulh ceza hâkimliğine başvuru yerine idare mahkemeleri nezdinde dava açılması usulü öngörülmüştür. Kanun'a eklenen geçiş hükmü gereği 1 Haziran 2024 tarihi itibarıyla sulh ceza hâkimlikleri önünde bulunan dosyalar, bu hâkimliklerce nihai karara bağlanacaktır. Son olarak, yurt dışı aktarımlara ilişkin Kanun'un mevcut hükümleri de yeni hükümlerle birlikte 1 Eylül 2024 tarihine kadar yürürlükte olmaya devam edecektir.



2. Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu Yayınlandı!

Kişisel Verileri Koruma Kurum'u ("Kurum") tarafından, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5/2-a maddesinde düzenlenen "*kanunlarda açıkça öngörülme*" kişisel veri işleme şartına dair Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu ("**Bilgi Notu**") 12.02.2024 tarihinde Kurum'un resmi internet sitesinde yayımlanmıştır. Bilgi Notu ile, kanunlarda açıkça öngörülmüş olması halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesini mümkün kılan "*kanunlarda açıkça öngörülme*" işleme şartının Türk ve Avrupa Birliği Hukuku kapsamında değerlendirilmesi yapılarak örnekler üzerinden uygulamadaki yansımalarına yer verilmiştir. Bilgi Notu'nda öne çıkan önemli değerlendirmeler kısaca şunlardır:

- Kişisel verilerin korunması, Anayasa'nın 20. maddesi kapsamında 2010 yılında yapılan değişiklik ile temel hak niteliği kazanmıştır. Bu doğrultuda, diğer tüm temel hak ve özgürlüklerde olduğu gibi, kişisel verilere ilişkin koruma mutlak değildir; Anayasa'nın 13. maddesindeki esaslara uygun olarak hakkın özüne dokunmadan "ancak" kanun ile sınırlandırılabilir. Bu minvalde, kişisel verilerin korunması hakkı kapsamında Kanun'un uygulanamayacağını öngören istisnai halleri düzenleyen 28. Maddesi, ilgili kişilerin bu hakkına yönelik kanun ile getirilen bir sınırlama teşkil etmektedir.
- Temel hak ve özgürlüklerin "ancak" kanun ile sınırlandırabileceğini öngören hükmün lafzı gereği, bu hak ve özgürlüklerin tüzük, yönetmelik, kanun hükmünde kararnameler gibi araçlar ile düzenlenmesinin veya sınırlandırılması mümkün değildir. Bu bağlamda Kurum, idarenin düzenleyici işlemleri ile doğrudan bir temel hak sınırlaması yapılamayacağını, diğer bir deyişle belli bir kanunun Anayasa'ya uygun olarak getirmiş olduğu sınırlama dışında yeni bir sınırlama yaratılamayacağını belirtmiştir. Örneğin, kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin Bilgi Teknolojileri ve İletişim Kurumu'na doğrudan düzenleme yetkisi veren düzenleme, yasama yetkisinin devredilemezliği ilkesi gereğince Anayasa Mahkemesi'nin 2013/122 E., 2014/74 K. sayılı kararı ile iptal edilmiştir.
- Ek olarak Kurum, temel hakkı güçlendirici ve hakkın daha etkin kullanılmasını sağlayan düzenlemelerin sınırlama olarak kabul edilemeyeceğinin, bu nedenle idarenin kanuni sınırlamaları somutlaştırarak düzenlemeler yapabileceğinin altını çizmiştir. Bu doğrultuda idare tarafından tesis edilen usulüne uygun yürürlüğe konulmuş düzenleyici işlemlerin iptal edilmediği sürece idari teşkilat içerisinde bağlayıcı olduğu ve uygulanması gerektiği ifade edilmiştir.
- Öte yandan, Kanun'un 5. maddesindeki "*kanunlarda açıkça öngörülme*" kişisel veri işleme şartına ilişkin hükmün dar veya geniş yorumlanması idarenin takdir yetkisi kapsamındadır; ancak bu takdirin temel hak ve özgürlükleri kısıtlamayacağı belirtilmiştir. Zira Kurum, hükümde belirtilen "açık" ibaresinin lafzi yorum yapılarak değerlendirilmesinin Kanun'un ruhuna aykırı olacağını ve söz konusu işleme şartının çok sınırlı hallerde uygulanabileceğini vurgulamıştır. Buna göre, kişisel veri işlenmesiyle ilgili herhangi bir kanunda açık bir hüküm varsa veya açık bir hüküm ile ikincil mevzuata yönlendirme yapılmışsa kişisel verilerin işlenmesi ancak o durumda mümkün olacaktır.
- Konuya ilişkin Avrupa Birliği Hukuku mevzuatları incelediğinde, GDPR'da her ne kadar Türk hukukundan farklı olarak "*kanunlarda açıkça öngörülme*" ve "*hukuki yükümlülüğün yerine getirilmesi*" hükümlerinin birbirinden ayrı düzenlenmediği belirtilse de, uygulamada benzer bir amaca hizmet ettiği görülmektedir.



- GDPR gerekçesi madde 41 uyarınca, veri sorumlusunun genel amacının, genel hukuk kurallarında veya özel bir kanunda yeterince açık bir temeli olan hukuki bir yükümlülüğe uymak olduğu kabul edilmiştir. Bu yükümlülük belirli bir kanuni hükme atıfta bulunarak veya onun uygulamasını açıkça ortaya koyan bir tavsiye, kurul kararı veya rehber gibi kaynaklara işaret ederek tanımlanabiliyorsa hukuki yükümlülük şartı olarak kabul edilecektir. Yine, İrlanda Veri Koruma Otoritesi tarafından yayımlanan “Kişisel Verilerin İşlenmesinin Hukuki Mesneti Rehber Notu” çalışmasına göre, hukuki hukuki yükümlülük işleme şartı birincil kanuni düzenlemeden kaynaklandığı gibi ikincil derecedeki mevzuatlar ile de işaret edilebilecektir.

3. Etkili Bir Ceza Soruşturması Yürütülmemesi Nedeniyle Kişisel Verilerin Korunmasını İsteme Hakkının İhlali Hakkında Anayasa Mahkemesi Kararı

Anayasa Mahkemesi (“AYM”), 22.03.2024 tarih ve 32497 sayılı Resmi Gazete’de yayımlanan 2020/36976 numaralı ve 13.02.2024 tarihli “Furkan Çakır Başvurusu Kararı” (“Karar”) ile, iş sözleşmesini fesheden işverenin işçilik alacaklarını ödememek için çalışanın (“Başvurucu”) bilgisi ve rızası dışında hesap hareketlerine erişmesi sebebiyle çalışan tarafından yapılan şikâyet hakkında etkili bir ceza soruşturması yürütülmemesi nedeniyle kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir.

Karara konu olayda Başvurucu, işvereni tarafından, şirket yetkisini kullanarak haksız kazanç elde etmekle itham edildiğini, işverenin kendisi hakkında yaptığı suç duyurusunda kendisine ait bir hesap hareketinin incelenmesini banka adı, miktar ve tarih belirterek talep ettiğini, kendisi hakkındaki kişisel verilere erişmeden anılan detayları bilmesinin mümkün olmadığını ileri sürerek 09.10.2020 tarihinde Samsun Cumhuriyet Başsavcılığına (“Başsavcılık”) suç duyurusunda

bulunmuştur. Başsavcılık, kişisel verilerin salt duyu organları vasıtasıyla öğrenilip başkalarına açıklanmasının kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunu oluşturmayacağı ancak şartları varsa özel hayatın gizliliğini ihlal suçunun değerlendirilebileceğini belirterek suçun şekli unsurlarının oluşmadığı gerekçesiyle kovuşturma yapılmasına yer olmadığına karar vermiştir. Bununla birlikte başvurusunun atılı suçun işlendiğine ilişkin soyut beyanından başka delil bulunmadığı ifade edilmiştir.

Başvurucu; şikâyet dilekçesinde bankalara müzekkere yazılmasına ve tanığının dinlenilmesine ilişkin talepte bulunduğunu, ayrıca kendisi hakkında yapılan suç duyurusuna ilişkin soruşturma dosyasının incelenmesini istediğini, buna rağmen soyut beyandan başka delil bulunmadığı gerekçesiyle takipsizlik kararı verildiğini belirterek anılan karara Samsun 1. Sulh Ceza Hâkimliği (“Sulh Ceza Hâkimliği”) nezdinde itiraz etmiştir. Sulh Ceza Hâkimliği ise anılan kararda isabetsizlik bulunmadığı gerekçesiyle itirazın reddine kesin olarak karar vermiştir. Bunun üzerine Başvurucu, kişisel verilerinin hukuka aykırı olarak ele geçirildiği şikâyeti hakkında etkili bir ceza soruşturması yürütülmediği iddiasıyla AYM’ye bireysel başvuruda bulunmuştur.

AYM ilk olarak, bir kişinin sadece kimliğini ortaya koyan bilgilerin değil, kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında değerlendirileceğini; bu doğrultuda banka ve kredi kartı hesap hareketlerinin kişisel veri olarak kabul edileceğini belirtmiştir. Anayasa’nın 20. maddesi uyarınca herkesin kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğunu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilmeyi, bu verilere erişmeyi, bunların düzeltilmesini veya silinmesini talep etmeyi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığını vurgulamıştır. Bu nedenle devletin, bireyin kişisel verilerinin korunması hakkına keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığını, bu bağlamda pozitif yükümlülüklerinin de olduğunu, bu anlamda uyuşmazlıkların çözümüne ilişkin etkili yargısal sistem kurma yükümlülüğünü yerine getirmesi gerektiğini belirtmiştir. Yapılan bu değerlendirmeler ile somut olayda, Başsavcılıkça başvurusunun ifadesi alınmadan ve şikâyet dilekçesinde ileri sürdüğü deliller toplanmadan dosya üzerinden karar verilmesi sonucu suç vasfının yanlış değerlendirildiği, Başvurucuya iddia ve delillerini ileri sürebileceği etkili bir hukuksal mekanizma sağlanmadığı, dolayısıyla usule ilişkin pozitif yükümlülüğün yerine getirilmediği sonucuna varılmıştır. Tüm bu nedenlerle AYM, Başvurucunun Anayasa’nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir. Bu doğrultuda Kararın bir örneği özel hayata saygı hakkı kapsamındaki kişisel verilerin korunması isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden soruşturma yapılmak üzere Samsun Cumhuriyet Başsavcılığına gönderilmiştir.

Sonuç olarak Karar ile, devletin kişilere iddia ve delillerini ileri sürebileceği etkili bir hukuksal mekanizma sağlaması gerektiğinin yanı sıra, bireyin kişisel verilerinin korunması hakkına keyfi müdahaleler ile üçüncü kişiler tarafından yapılan saldırıları da önlemekle yükümlü olduğu vurgulanmıştır.

4. Kişisel Verilerin Korunmasını İsteme Hakkı Kapsamında Cumhurbaşkanlığı Kararnamesi Hükümlerinin İptaline İlişkin Anayasa Mahkemesi Kararı

Anayasa Mahkemesi ("AYM"), 27.02.2024 tarih ve 32473 sayılı Resmî Gazete'de yayımlanan 2018/118 E. ve 2023/180 K. sayılı ve 26.10.2023 tarihli kararı ("Karar") ile, 1 Numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin ("Kararname") çeşitli hükümlerini, Anayasa'nın 20. maddesi uyarınca güvence altına alınan kişisel verilerin korunmasını isteme hakkı kapsamında iptal etmiştir.

AYM ilgili Kararında, Cumhurbaşkanlığı Kararnamesi ile getirilen düzenlemelerin Anayasa'nın İkinci Kısımının Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümü'nde yer alan siyasi haklar ve ödevler ile Anayasa'da münhasıran kanunla düzenlenmesi öngörülen ya da kanunda açıkça düzenlenen konulara ilişkin olmaması gerektiğini belirtmiştir. Bu doğrultuda, Anayasa'nın "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünde yer alan kişisel verilerin korunması hakkına ilişkin olarak düzenleme yapılmasının mümkün olmadığını belirterek Kararname'nin çeşitli hükümlerini iptal etmiştir. İptal edilen hükümler ile iptal gerekçeleri aşağıda kısaca özetlenmiştir:

- Kararname'nin 8. maddesinin (f) fıkrasında yer alan ve Cumhurbaşkanlığı İdari İşler Başkanlığının birimlerinden biri olan Personel ve Prensipler Genel Müdürlüğü'nün görevleri arasında sayılan "Devletin sevk ve idaresinde görevli üst kademe yöneticileri hakkında bilgi toplamak, sicil özetlerini ve biyografilerini tutmak" hükmündeki "bilgi toplamak" ibaresi iptal edilmiştir. AYM iptal gerekçesinde, devletin sevk ve idaresinde görevli üst kademe yöneticileri hakkında toplanacak bilgilerin kişilerin mesleki ve özel durumlarını yansıtan sicil bilgileri, iş ve sosyal yaşamını içine alacak şekilde özgeçmişleri gibi kişisel veri niteliği taşıyan bilgilerden oluşacağını vurgulayarak; kişisel verilere ilişkin bu düzenlemenin Cumhurbaşkanlığı Kararnamesi ile düzenlenemeyecek yasak alan içinde kaldığını belirtmiştir.
- Cumhurbaşkanlığı politika kurullarının çalışma usul ve esaslarına düzenleyen Kararname'nin 33. maddesinin 3. fıkrasında yer alan "Kurullar, kendi görev alanlarıyla ilgili olarak her türlü bilgi ve belgeyi ilgili bakanlıklar ile kamu kurum ve kuruluşlarından talep edebilir. Söz konusu talepler kurum ve kuruluşlarca öncelikle değerlendirilir." hükmünde yazılı "her türlü bilgi ve belgeyi" ibaresi ile Cumhurbaşkanlığı politika kurullarının bilgi toplama ve sır saklama yükümlülüğünü düzenleyen 36. maddesinde yer alan "Kurullar, görevleri ile ilgili olarak gerekli olan bilgileri bütün kamu kurum ve kuruluşlarından istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları bu bilgileri vermekle yükümlüdürler." hükmünde yazılı "gerekli olan bilgileri" ibaresi nedeniyle ilgili fıkra ve madde iptal edilmiştir. AYM gerekçesinde, her türlü bilgi ve belge ile gerekli olan bilgiler ibarelerinin kapsamında kişisel verilerin de bulunduğu bahisle ilgili hükümlerin Cumhurbaşkanlığı Kararnamesi ile düzenlenemeyecek yasak alan içinde kaldıklarını belirtmiştir.
- Kararname'nin on üçüncü bölümü kapsamında, Sağlık Bakanlığı'nın bilgi toplama, işleme ve paylaşma yetkisini düzenleyen 378. maddesi, kuralın sağlık hizmetleriyle ilgili olarak kişisel verilerin toplanmasına, işlenmesine, aktarılmasına, bu kişisel verilere erişim sisteminin kurulmasına, sistemin güvenliğinin sağlanmasına ilişkin düzenlemeleri içermesi nedeniyle Cumhurbaşkanlığı Kararnamesi ile düzenlenemeyecek yasak alan dahilinde olduğu vurgulanarak iptal edilmiştir. İptal kararının hukuki boşluk doğurmaması adına, 9 ay sonra yürürlüğe girmesine karar verilmiştir.

Sonuç olarak Karar ile Anayasa'nın 20. maddesi uyarınca güvence altına alınan kişisel verilerin korunmasını isteme hakkının Anayasa'nın "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünde yer alan temel haklardan olduğunun, bu nedenle Cumhurbaşkanlığı Kararnamesi ile bu hak kapsamında düzenlemelerin getirilemeyeceğinin altı çizilmiştir.

5. Türkiye ve Dünya'dan Güncel Haberler!

i. Türkiye

- ⇒ Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Birleşmiş Milletler Kalkınma Programı (UNDP) iş birliği ile Türkiye'de veri erişimini, kullanımını ve paylaşımını tanımlayacak olan bir yönetim çerçevesi oluşturulması amacıyla "[Veri Yönetişimi Çerçevesi - Türkiye için Tavsiye Raporu](#)" yayımlandı. Bu çalışma haricinde Ulusal Veri Stratejisi hazırlıkları kapsamında, açık devlet verisi, veri yerelleştirme ve ulusal veri sözlüğüne yönelik mevzuat çalışmaları ile yapay zekâ veri yönetişimi ihtiyaçlarına yönelik kapsamlı ihtiyaç analizi ve öneri raporu için de çalışmalarının devam ettiği aktarıldı. Tüm paydaşların katkıları ve görüş alma süreci sonrasında nihai taslak hale gelecek Ulusal Veri Stratejisi'nin ise 2025 yılı başında tamamlanacağı belirtildi.
- ⇒ Rekabet Kurulu tarafından, META Platforms, Inc. ("META") hakkında, Threads ve Instagram uygulamalarını bağlamak suretiyle hâkim durumunu kötüye kullandığı şüphesi üzerine başlatılan soruşturmada [geçici tedbir kararı](#) verildi. META'nın, Instagram hesaplarına dayalı Threads profili oluşturan kullanıcıların verilerini, kullanıcılara onay seçeneği sunmaksızın birleştirmesinin; soruşturma tamamlanana kadar tafisi güç zararlara yol açacağı değerlendirildi. META'nın metin tabanlı sosyal medya platformu Threads, Rekabet Kurulu'nun tedbir kararına uymak için 29 Nisan'dan itibaren Türkiye'de kapatılacak.





- ⇒ Ticaret Bakanlığı'na bağlı olan Reklam Kurulu, "Dijital Tüketicinin Korunması Projesi" kapsamında e-ticaret sitelerini mercek altına alarak, kullanıcıların üyelikten çıkmalarını zorlaştıran, kişisel verileri üçüncü kişilerle paylaşan, hedefli reklamcılık yapan ve ticari ileti onayı iznini zorunlu tutan, aralarında Amazon Türkiye de bulunan 12 e-ticaret platformu hakkında [idari para cezası, durdurma ve düzeltme yaptırımlarını uyguladı](#). Reklam Kurulu yaptığı incelemeler sonucu firmaların üyelik sözleşmeleri ile aydınlatma, açık rıza ve çerez politikası gibi çeşitli metinlerini de analiz ederek, tüketicilerin karar verme veya seçim yapma iradesinin olumsuz etkilendiğini ve tüketicilerin açıkça bilgilendirilmediğini, bu gibi durumların yanıltıcı nitelikte olduğunu ve dürüst rekabet ilkelerine aykırılık teşkil ettiğini belirtmiştir.

ii. Dünya

- ⇒ Birleşik Krallık Veri Koruma Otoritesi ("ICO"), ceza verme yetkisini nasıl kullandığı konusunda şeffaflığı arttırmak adına cezaların nasıl verileceğini ve para cezalarının nasıl hesaplanacağını belirleyen yeni [veri koruma ceza kılavuzunu](#) yayınladı. Kılavuzda ICO'ya para cezası uygulama yetkisi veren yasal çerçeve, bir teşebbüs veya kuruluşun ekonomik varlığının tanımlanmasına ilişkin yaklaşımlar ile uygulanacak idari para cezasının hesaplanmasında kullanılan metodolojiye yer verilmiştir.
- ⇒ Dünya genelinde yapay zekânın risklerini sınırlamaya yönelik dünyanın ilk kapsamlı çerçevesini sunan Yapay Zekâ Yasası (AI Act) çeşitli yasal süreçlerin ardından 13.03.2024 tarihinde Avrupa Parlamentosu tarafından [onaylandı](#). Söz konusu metnin "düzeltme prosedürü (corrigendum)" olarak adlandırılan hukuki dil incelemesinden geçirilmesinin ardından, Avrupa Konseyi'nin resmi onayı ile Avrupa Birliği Resmî Gazetesinde (EUR-Lex) yayımlanmasını takip eden yirminci günde yürürlüğe girecektir.
- ⇒ Fransa Veri Koruma Otoritesi (Commission nationale de l'informatique et des libertés "CNIL") tarafından, kişisel verilerin güvenliğinin sağlanmasına yönelik [2024 yılı Kişisel Veri Güvenliği Rehberi](#) yayımlandı. Bahse konu Rehberde; özellikle yapay zekâ, mobil uygulamalar, bulut bilişim ve uygulama programlama ara yüzleri (API) ile bu alanlar

kapsamında kişisel verilerin nasıl işlenmesi gerektiği konularına odaklanılmaktadır. Ayrıca CNIL, çok faktörlü kimlik doğrulama çözümlerinin Avrupa Veri Koruma Tüzüğü'ne uygun olmasını sağlamak adına 31 Mayıs'ta sona erecek kamuya açık bir [istişare](#) başlattığını duyurdu.

- ⇒ Avrupa kurumlarının gizlilik ve veri koruma yasalarını desteklemesini sağlayan bağımsız bir denetim otoritesi olan Avrupa Veri Koruma Denetçisi (EDPS), Avrupa Komisyonu'nun ("Komisyon") Microsoft 365 kullanımı ile GDPR'da yer alan birtakım temel veri koruma düzenlemelerini ihlal ettiğini [belirtti](#). Bu kapsamda; Microsoft 365 kullanılırken hangi tür kişisel verilerin toplanacağını ve bunların hangi amaçlar doğrultusunda kullanılacağını veri sorumlusu Komisyon ile Microsoft arasında akdedilen sözleşmede yeterli şekilde gösterilmediği, kişisel verilerin aktarımında mevzuat hükümlerinin ihlal edildiği, bu bağlamda yeterlilik kararı kapsamında olmayan ülkelere yapılacak aktarımın 9 Aralık 2024 tarihinden itibaren geçerli olmak üzere durdurulması yönünde Komisyonun talimatlandırılmasına karar verildiği belirtildi.
- ⇒ AB Konseyi ve Avrupa Parlamentosu, AB düzeyinde sağlık verilerinin paylaşımını ve bunlara erişimi kolaylaştıracak yeni bir yasa üzerinde geçici bir [anlaşmaya vardı](#). Avrupa Sağlık Veri Alanı (EHDS) için önerilen düzenleme, bireylerin kişisel elektronik sağlık verilerine erişimini ve bu veriler üzerindeki kontrolünü geliştirmeyi ve aynı zamanda belirli verilerin kamu yararı, politika desteği ve bilimsel araştırma amaçları için yeniden kullanılmasını sağlamayı amaçlamaktadır.
- ⇒ Almanya Sağlık Bakanlığı, [Sağlık Verileri Kullanım Yasası](#)'nın 26 Mart'ta yürürlüğe girdiğini duyurdu. Yasa ile, ilaç şirketlerine araştırma amacıyla hastaların sağlık verilerine erişim izni vererek sağlık araştırmalarının ilerletilmesi amaçlanmaktadır. Bu doğrultuda araştırmacıların kullanımına sunulan veriler anonimleştirilecek ve hasta mahremiyetinin ihlal edilmesi halinde idari para cezaları uygulanacaktır.
- ⇒ Florida eyaletinde, çocuklara yönelik en katı sosyal medya yasaklarından birini öngören yasa [resmileşti](#). 1 Ocak 2025'te yürürlüğe girecek olan düzenleme, sosyal medya platformlarını aşırı kullanan çocukların zihinsel sağlığı üzerindeki zararlı etkilerin ortadan kaldırılması ve bunun sonucunda kaygı, depresyon ve diğer akıl hastalığı risklerinden korunmalarını amaçlamaktadır. Düzenlemenin kapsamını, *sonsuz kaydırmayı* destekleyen, beğeniler gibi tepki ölçümlerini görüntüleyen, otomatik oynatılan videolar içeren ve canlı yayın ve anlık bildirimlere sahip sosyal medya platformları oluşturmaktadır.



⇒ Amerika Birleşik Devletleri (“**ABD**”) Senatosu tarafından, Pekin merkezli Bytedance şirketinin ana ortağı olduğu TikTok’un devredilmesinin, devredilmemesi halinde ise yasaklanmasının önünü açan yasa tasarısı [onaylandı](#). ABD Temsilciler Meclisi, 13 Mart’ta yaptığı oylamada, "Amerikalıları Yabancı Düşmanlarca Kontrol Edilen Uygulamalardan Koruma Yasası" başlıklı tasarımı büyük çoğunlukla kabul ederek onaylanması için ABD Senatosuna göndermişti. ABD Başkanı Joe Biden ise, Senato’nun onaylaması halinde yasayı imzalayarak yürürlüğe koyacağını bildirmişti. Ulusal güvenlik tehdidi oluşturduğu gerekçesiyle TikTok’un yasaklanmasının önünü açan tasarının yasalaşması halinde, ana ortak konumundaki ByteDance, platformu devretmek zorunda kalacaktır. Aksi takdirde TikTok’un ABD’deki internet uygulama mağazalarından 5 ay süreyle veya tamamen çıkarılması öngörülmektedir.

Herhangi bir sorunuz olması halinde bizlerle her zaman iletişime geçebilirsiniz.

İletişim

Burçak Kurt Biçer

Yönetici Ortak

burcak.bicer@bicerguner.com

Uğurkan Şeber

Kıdemli Avukat

ugurkan.seber@bicerguner.com

İrem Efe

Avukat

irem.efeb@bicerguner.com