TORUN HUKUK BÜROSU
torunhukukburosu@gmail.com

Cevizlidere Mah. 1219. Sok.
No:2 Latif Apt.D.3 Balgat
06520 Çankaya/ANKARA

Telefon : 0 312 432 56 78
Mobil : 0 553 707 43 26

Kişisel Verilerin Korunması Hukuku Bülteni
Law Bulletin of Personal Data Protection

Bülten (Bulletin) No:1 Ekim(October) 2020

İçindekiler (Contents)

Konular/Subjects	Sayfa/ Page
Kişisel Verilerin Korunması Alanında Hukuk Büromuz Tarafından Gerçek ve Tüzel Kişilere Verilebilecek Hukuki Destek ve Danışmanlık *Legal Support and Consultancy Provided by Our Law Office to Natural and Legal Persons in the Field of Personal Data Protection*	2
Kişisel Verilerin Korunmasına Yönelik Türk Ceza Kanununda ve Kişisel Verilerin Korunması Kanununda Mevcut Yaptırımlar ile Bu Yaptırımlara Karşı Hukuki Çareler *Sanctions actuelles pour la protection des données personnelles dans le Code pénal turc et dans la loi sur la protection des données personnelles et recours juridiques contre ces sanctions*	9
Kişisel Verilerin İşlenmesine Egemen Olan İlkeler ve Bu Kapsamda Verilen KVK Kurulu Kararları *Principles Governing the Processing of Personal Data and Board Decisions Made Within This Scope*	22
İnternet Ortamında Yayınlanan İçeriklerin Kaldırılması veya Bu İçeriklere Erişimin Engellenmesi *Removing or Blocking Content Published on The Internet*	28
İşçi ile İşveren İlişkisi Bağlamında Kişisel Verilerin Korunması *Personal Data Protection in Labor Law Relations*	33
Tüzel Kişilerin (Anonim Şirket, Limited Şirket ve Diğer Şahıs Şirketlerinin) Veri Sorumluları Sicili'ne (VERBİS'e) Kayıt Süreci *The Enrollment Process of Legal Persons (Corporations, Limited Companies and Partnerships) to the Data Controllers Registry (VERBIS)*	40
Yurtdışında Yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü'ne dair Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Kararının İncelenmesi *Review of The Decision Dated 23.07.2019 and Numbered 2019/225 Issued by the Personal Data Protection Board*	44
Kişisel Verilerin Korunması Kanunu Çerçevesinde Türkiye'den Yurt Dışına Kişisel Veri Aktarımı *Foreign Direct Investment and Personal Data Transfer Abroad Within The Framework of The Law on The Protection of Personal Data in Turkey*	47
Sosyal Ağ Sağlayıcılarının Yükümlülükleri ve Bu Yükümlülüklere Aykırı Davranılması Halinde Uygulanacak Yaptırımlar *The Obligations of Social Network Providers and Sanctions to Be Applied in Case of Breach*	52

Kişisel Verilerin Korunması Alanında Hukuk Büromuz Tarafından Gerçek ve Tüzel Kişilere Verilebilecek Hukuki Destek ve Danışmanlık

Av.Erdem Arda Akay

Genel Olarak

❑ Gelişen ve değişen teknolojiyle birlikte sosyal ve ekonomik alanda yaşanan dönüşüm sonucu bir hizmetin sunumu, bir görevin yerine getirilmesi vb. etkileşimlerle bağlantılı olarak bireylere ilişkin veriler gerçek ve tüzel kişiler tarafından elde edilmektedir. Sosyal ve ekonomik alanda uzun yıllardır işlenmekte olan kişisel verilere ilişkin hukuk alanında da yapılan çeşitli çalışmalar sonucu kişisel verilerin işlenmesi ve korunması hususu kanuni bir zemine oturtulmuştur. 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu ile birlikte gerçek ve tüzel kişilerin etkileşimde oldukları kişilere ait kayıt altına alınan verilerin nasıl işlenebileceği düzenlenmiştir. 6698 sayılı bu Kanun, 95/46/EC Sayılı Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Direktifi, daha sonra yayımlanarak yürürlüğe giren ve direktifin yerini alan AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile 28 Ocak 1981 tarihinde Strazburg'da imzalanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ile uyumlu bir yasal düzenlemedir.

Veri sorumlusu ve veri işleyenler kimdir ?

❑6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi ile veri sorumlusu ve veri işleyen kavramları da kişisel verilerin korunması bağlamında hayatımıza girmiştir. Kimlerin veri sorumlusu, kimlerin ise veri işleyen konumunda olduğunu kanun açıkça ortaya koymuş ve gri alan bırakmamaya özen göstermiştir. 6698 sayılı Kanun'da veri sorumlusu "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanırken veri işleyen ise "Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak gösterilmiştir. Bu iki kavram kimi durumlarda aynı gerçek ve tüzel kişide birleşebileceği gibi yaygın olarak ayrı iki gerçek veya tüzel kişi olarak da karşımıza çıkabilmektedir. Buradaki temel ayrım; veri sorumlusu kişisel verilerin elde edilmesinden saklama süresinin sona ermesine kadar geçen süre içerisinde eldeki kişisel veriler üzerindeki her türlü işleme ve eyleme ilişkin karar alma yetkisine sahip kişiyken veri işleyen, veri sorumlusunun fiili hakimiyeti altında onun direktiflerini yerine getiren gerçek veya tüzel kişidir.

Legal Support and Consultancy Provided by Our Law Office to Natural and Legal Persons in the Field of Personal Data Protection

Introduction

❑ In connection with economic and technologic improvement, data on individuals are collected by natural and legal persons. This data collection can be done by way of performing a task or providing a service. This situation also affected the legal field. With the Law on Protection of Personal Data published in the Official Newspaper on April 7, 2016 and numbered 29677, a legal framework for the protection of recorded personal data belonging to individuals with whom natural and legal persons interact. The Law on Protection of Personal Data numbered 6698 complies with General Data Protection Regulation (on April 27, 2016 and numbered 2016/679) and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data(on January 28,1981 and numbered 108).

Who are the data controllers and data processors?

❑ With the enactment of the Personal Data Protection Law No.6698, the concepts of data controller and data processor have also entered our lives in the context of the protection of personal data. The law clearly states who is the data controller and who is the data processor and has taken care not to leave a gray area. In Law No. 6698, the data controller is defined as "the natural or legal person who determines the purposes and means of processing personal data, and is responsible for the establishment and management of the data recording system", while the data processor is "the natural or legal person who processes personal data on behalf of the data controller" shown as. In some cases, these two concepts can be combined in the same natural and legal person, or they can also be encountered as two separate natural or legal persons. The main distinction here is while the data controller is the person who has the authority to make decisions regarding all kinds of processing and action on the personal data in the period from the acquisition of the personal data until the end of the storage period, the data processor is the natural or legal person who fulfills his instructions under the actual control of the data controller.

Örneğin; satış ve pazarlama alanında faaliyet gösteren bir X firması, piyasaya sürülen ürünün hedeflenen müşteri kitlesi üzerindeki etkisini ve bu etkinin satış oranlarına yansımasını tespit etmek için bir araştırma şirketiyle çalışmaktadır. Yapılacak saha araştırmasında hedeflenen müşteri kitlesinin kimler olacağı, bu kişilerden hangi kişisel verilerin toplanacağı, toplanan verilerin ne süreyle işlenip saklanacağı X firmasının tasarrufundadır ve X firması veri sorumlusu olarak nitelenecektir. Araştırma şirketi ise ancak X firmasının talimatları doğrultusunda araştırmayı gerçekleştirebilmektedir ve kişisel verilerin işlenmesi bağlamında veri işleyen konumundadır.

Kişisel Verilerin Korunması Bağlamında Hukuk Büromuz Tarafından Hangi Hizmetler Sunulabilmektedir ?

❑ Yürürlüğe giren kanun sonrası veri sorumlusu sıfatını alan tüzel kişiler bakımından bunun en önemli sonucu olarak veri sorumlusu şirket ve kuruluşlara, kanuna göre Veri Sorumluları Siciline kaydolma zorunluluğu getirilmiştir. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisnalar getirilebilmektedir.

❑ Tüzel kişiler bakımından, 2016 yılında yürürlüğe giren KVK Kanunu'na uyum süreci, yerine getirilmesi gereken birtakım prosedürleri içermektedir. Bu aşamada ilk olarak karar verilmesi gereken, hayata geçirilecek uyum projesinin kapsamına, şirketin de hacmini göz önünde bulundurarak, karar vermek ve uyum projesinin kimlerle yürütüleceğini belirlemektir. Kişisel verilerin işlenmesi veri sorumluları açısından tek seferlik bir iş değil; faaliyetleri kapsamında sürekli olarak gerçekleştirmek zorunda oldukları bir işlemdir. Bu sürekliliğin sağlanabilmesi ve atılan adımların kanuna uygun olabilmesi adına hukukçu uzmanlardan ve veri güvenliği uzmanlarından yardım alınması isabetli olacaktır.

❑ Kişisel Verilerin Korunması alanında çalışan hukuk büromuzun yaptığı iş temel olarak müvekkilin yetkili merciler önünde temsili ve kişisel verilerin korunmasına ilişkin kendilerine danışmanlık sağlanmasıdır. Bu temsil ve danışmanlık kimi zaman geçici ve kısa süreli bir sorun üzerine gerçekleştirilirken, kimi zaman ise şirketler açısından geniş kapsamda kişisel veri mevzuatına uyum projeleri yürütmek şeklinde de hayata geçebilmektedir. Somut durum ne olursa olsun uzman avukat kadromuz, müvekkilin çıkarları doğrultusunda onun lehine olabilecek şekilde hareket edecek ve hayata geçirilmek istenen plan ve stratejilerin yasal sınırlar çerçevesinde gerçekleştirilebilmesine yardımcı olacaktır.

❑ *Gerek gerçek kişiler gerek ise şirketler ve kurumlar bazında, kişisel verilerin korunması alanında çalışan*

For example; A company X, operating in the field of sales and marketing, works with a research company to determine the impact of the product launched on the targeted customer base and the reflection of this effect on sales rates. "Who will be the targeted customer mass in the field research to be conducted?", "What personal data will be collected from these people?", "How long will the collected data be processed and stored ?" topics are at the disposal of X company and company X will be qualified as the data controller. The research company, on the other hand, can only carry out the research in line with the instructions of the X company and is in the position of data processor in the context of processing personal data.

Lawyers Role in Protection of Personal Data Law

❑ After the law, the most important consequence of this area is obligation to register with the Data Controller Registry for data controller legal entities. However, taking into account the objective criteria to be determined by the Board, such as the nature and number of the personal data processed, whether the data processing originates from the law or the status of transfer to third parties, the Board may make exceptions to the obligation to register in the Data Controllers Registry.

❑ In terms of legal entities, the process of compliance with the law, which entered into force in 2016, includes a number of procedures to be fulfilled. At this stage, the first thing to decide is to decide on the scope of the adaptation project to be implemented, taking into account the size of the company, and to determine with whom the harmonization project will be carried out. The processing of personal data is not a one-off job for data controllers; It is a process that they have to perform continuously within the scope of their activities. It would be appropriate to seek help from legal experts and data security experts in order to ensure this continuity and to ensure that the steps taken are legal.

❑ The task of our lawyers and our law firm working in the field of Protection of Personal Data is primarily to provide consultancy to the client before the competent authorities regarding the representation and protection of personal data. This representation sometimes short time, sometimes take long time for conducting projects for compliance with personal data legislation for companies. Our lawyers and law firm working in Protection of Personal Data, will act in favor of the client in the interests and will help to realize the plans and strategies that are desired to be implemented within the legal limits.

❑ *Consultancy and services offered by our law firm working in the field of personal data protection can be counted as follows:*

avukatlarımız tarafından sunulan danışmanlık ve hizmetler şu şekilde sayılabilir:

Kişisel Verilerin Korunması Kanunu'nun Gereklerine Uygun ve Kapsamlı Bir Strateji Geliştirmek

❑ Gerçek ve tüzel kişilerin, bünyesinde çalışan kişilerin ve müşterilerinin kişisel veri niteliğindeki bilgilerini kendi sistemlerine işleyebilmeleri Kişisel Verilerin Korunması Kanunu ile çizilen sınırlar dahilinde gerçekleştirilebilecektir. Bu kapsamda gerçek ve tüzel kişiler Kişisel verilerin işlenmesinde göz önünde bulundurulması gereken birtakım ilkeler mevcuttur. Buna göre kişisel verilerin işlenmesi işlemi hukuka ve dürüstlük kuralına uygun yapılmalı; işlenen veriler doğru ve güncel olmalı; veriler belirli, açık ve meşru amaçlar için işlenmeli; işlendikleri amaçla sınırlı ve ölçülü olmalı; işlenen veriler ilgili mevzuatta öngörülen ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

❑ Bu ilkelere aykırı bir veri işleme yapılması halinde veri sorumlusu şirket idari ve cezai yönden sorumluluk altına girecektir. Böyle bir zarardan kaçınmak ve mevzuata uygun bir veri işleme süreci yürütmek adına konunun uzmanı bir avukatla çalışıp veri sorumlusu şirkete uygun bir veri işleme stratejisi belirlenmesi isabetli olacaktır. Önemle belirtmek gerekir ki kişisel verilerin işlenmesine ilişkin belirlenecek strateji, yaptırımlara karşı günü kurtaracak bir hamle değil; tüzel kişiliğin veri işlenmesine ilişkin sahip olacağı geleneğin ilk adımını atmak olacaktır.

Müşterilerin Verilerinin Gizlilik Sözleşmelerine ve Açık Rızaya Dayanmasına, Verilere Erişim Prosedürlerine ve Aydınlatma Yükümlülüğüne İlişkin Gerekli Belgelerin Hazırlanması

❑ Kanun veri sorumlusu olarak gerçek veya tüzel kişi ayrımı yapmasa da kişisel verileri koruma altında olan kişiler, yani kanunun nitelendirmesiyle "ilgili kişi", ancak gerçek kişiler olabilmektedir. Bu bağlamda tüzel kişilik bünyesinde çalışan veya tüzel kişiyle etkileşime giren gerçek kişilere ilişkin de yerine getirilmesi gereken bazı yükümlülükler mevcuttur. Öncelikle, kişisel verileri işlenecek olan gerçek kişilerin bu işleme dair açık rızalarının alınması gerekmektedir. Anayasamızın 20.maddesinin 3.fıkrasında, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği hüküm altına alınmıştır. Yalnızca kanunda sayılan hallerde açık rıza bulunmadan veri işleme yapılabilecektir.

❑ Açık rıza; belirli bir konuya ilişkin, bilgilendirilmeye dayanan, özgür irade açıklamasıdır. Bu anlamda açık rıza alınmasının ilk boyutu bilgilendirme boyutudur. Kişisel verileri işlenecek ilgili kişi sürece dair bilgilendirilmeli, ondan sonra rızasına başvurulmalıdır. Açık rızanın alınmasına ilişkin bir şekil şartı bulunmamasına karşılık ispat gücü bakımından bu rızanın yazılı veya elektronik ortamda alınması veri sorumluları açısından isabetli olacaktır.

Developing an overall strategy for complying with data protection requirements

❑ Natural and legal persons will be able to process the personal data of their employees and customers within the limits set by the Personal Data Protection Law. There are some principles to consider about processing personal data. The processing of personal data should be done in accordance with the law and the honesty rule; the processed data must be accurate and up-to-date; data should be processed for specific, clear and legitimate purposes; be limited and restrained for the purpose for which they are processed; processed data should be maintained for the period required by the relevant legislation or for the purpose for which they are processed.

❑ In case of failure to comply with these rules, the data controller will be under administrative and criminal liability. Working with lawyers or law firms which have experience in data protection would be helpful to avoid this situation. It should be emphasized that the strategy to be determined for the processing of personal data is not a move to save the day against sanctions; It will be to take the first step in the tradition of the legal entity regarding data processing.

Drafting necessary documents, in particular employee privacy policies, access procedures

❑ Clear consent of natural persons whose personal data will be processed must be taken. Data can only be processed without explicit consent in cases specified in the law. Before take the clear consent, the person whose personal data will be processed should be informed about the process. However, within the framework of the privacy policy with the data subjects, the contract will be signed stating that the personal data obtained will not be shared with third parties. This issue is very important for the fundamental rights and freedoms of the person and should be taken into consideration by the data responsible clients in order not to cause violations of rights.

(***) Önemle belirtmek gerekir ki, herhangi bir ürün ve/veya hizmetin sunumu, açık rıza verme ön şartına bağlanamayacaktır. Yapılan seçimin sonuçları kişisel veri ilgilisinin seçim özgürlüğünü etki altında bırakıyorsa bu durumda ilgili kişi tarafından verilen rızanın özgürce verildiğini söylemek mümkün olamayacaktır.

❑ Açık rıza her ne şekilde alınacak olursa olsun, Kanun'un açık rızayı şart koştuğu durumlarda bu durum beraberinde aydınlatma yükümlülüğünü de getirecektir. Aydınlatma yükümlülüğü, veri sahibinin haklarına ilişkin şeffaf bilgilendirme olarak tanımlanabilecektir. Açık rızanın meydana gelebilmesinin üç şartından biri olan bilgilendirmeye dayalı olma hususundan, ancak aydınlatma yükümlülüğünün gereği gibi yerine getirilmesi sonucu söz edilebilecektir. ***Aydınlatma Yükümlülüğü'nün Yerine Getirilmesinde Uyulacak Usul ve Esas Hakkında Tebliğ*** 10 Mart 2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

❑ Veri sorumluları veya yetkilendirecekleri kişiler tarafından yerine getirilecek aydınlatma yükümlülüğünde asgari olarak; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kimlere ve hangi amaçla aktarılabileceği, kişisel verilerin toplanmasında benimsenecek yöntem ve hukuki sebebi, kişisel verisi toplanacak ilgili kişinin 6698 sayılı Kanun'un 11.maddesinde sayılan diğer haklarına dair bilgilendirme yapılmalıdır. Yükümlülüğü yerine getirirken kullanılacak metnin amaca uygun, açık, belirli ve meşru olması gerekmekte ve muğlak ifadelerden kaçınılarak sade ve anlaşılır bir dilin benimsenmesi önem arz etmektedir. Böylece ilgili kişi, kendisine dair işlenecek verinin ne amaçla ve ne şekilde işlenebileceğine dair bilgi sahibi olabilecek ve vereceği açık rıza özgür iradesinin ürünü olabilecektir.

(***) Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir ve bununla ilgili olarak yaşanabilecek uyuşmazlıkta aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.

❑ Aydınlatma yükümlülüğü sonucu elde edilen açık rızanın yanı sıra verileri işlenen ilgili kişilerle gizlilik politikası çerçevesinde, elde edilen kişisel verilerin üçüncü kişilerle paylaşılmayacağına ilişkin sözleşme imzalanacaktır. Bu husus kişi temel hak ve hürriyetleri açısından son derece önemlidir ve hak ihlallerine yol açmamak adına veri sorumlusu müvekkiller tarafından göz önünde bulundurulmalıdır.

(***) *** It should be emphasized that the presentation of any product and / or service cannot be bound by the precondition of express consent. If the results of the selection affects the freedom of choice of the personal data subject, then it will not be possible to say that the consent given by the data subject is freely given.

❑ Regardless of the way express consent will be obtained, in cases where the law stipulates explicit consent, this situation will bring along the obligation to inform. Obligation to inform can be defined as transparent information regarding the rights of the data owner. One of the three conditions for the occurrence of explicit consent, being based on information, can only be mentioned as a result of duly fulfilling the obligation to inform.

❑ As a minimum in the obligation to inform to be fulfilled by the data controllers or the persons they authorize; Identity of the data controller and its representative, if any, the purpose for which the personal data will be processed, to whom and for what purpose it can be transferred, the method and legal reason to be adopted in the collection of personal data, and other rights of the person whose personal data will be collected, enumerated in Article 11 of Law No. 6698. While fulfilling the obligation, the text to be used must be suitable for the purpose, clear, specific and legitimate, and it is important to adopt a plain and understandable language by avoiding ambiguous expressions. Thus, the relevant person will be able to have information about what purpose and how the data to be processed can be processed, and the explicit consent to be given can be the product of his free will.

(***) Fulfillment of the obligation to inform doesn't depend on the request of the person concerned, and the proof of fulfillment of the disclosure obligation in case of any dispute related to it belongs to the data controller.

❑ In addition to the express consent obtained as a result of the obligation to inform, a contract will be signed with the relevant persons whose data is processed, stating that the personal data obtained will not be shared with third parties within the framework of the privacy policy. This issue is extremely important in terms of fundamental rights and freedoms of the person and should be taken into consideration by the data controller clients in order not to cause violations of rights.

Kişisel Verilerin Korunması Kurumu'na Yapılacak Veri Bildirimi ve Diğer İşlemlere İlişkin Başvuruların Hazırlanması

❑ Kanunda veri sorumlusu olarak adlandırılan gerçek ve tüzel kişiler, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Gerçek ve tüzel kişiler, veri bildiriminde bulunulmadan önce Veri Sorumluları Sicili'ne kaydolmak zorundadır. Kişisel Verilerin Korunması Kurumu bünyesindeki bu sicile kaydolan veri sorumluları, müşterilerine ve çalışanlarına dair elinde bulunan kişisel veriler hakkında bu sicile bildirimde bulunacaktır. Bununla birlikte veri sorumlularının kişisel verilere ilişkin beyanları, şikayetleri ve diğer işlemler için de Kurum'a başvuru yapılacaktır. Yapılacak olan veri bildirimi ve diğer başvuruların usule uygun gerçekleştirmesi önem arz etmektedir. Bu nedenle sürecin bu alanda çalışan avukatlar tarafından yürütülmesi olası hak kayıplarının önüne geçebilecektir.

Prepare regulatory filings, including notification of data processing to the DPAs

❑ Natural and legal persons, who are named as data responsible in the law, refer to the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system. They must register with the Data Controllers Registry before data can be reported. The data officers registered in this registry within the body of the Personal Data Protection Institution will notify this registry about the personal data available to their customers and employees. In addition, applications will be made to the institution for the statements, complaints and other transactions of the data responsible for personal data. It is important that data reporting and other applications are made duly. For this reason, the process to be carried out by lawyers working in this field will prevent possible loss of rights.

Çalışanların Verilerinin Korunması Hakkında Şirket ve Kurumlara Danışmanlık Verilmesi, Eğitim Programlarının Düzenlenmesi

❑ Kişisel verilerin korunması bağlamında hayata geçireceğimiz uyum süreci projesi yalnızca Kurum'a yapılacak bildirim ve başvurularla sınırlandırılmamalıdır. Ülkemizde henüz son yıllarda gelişmekte olan kişisel veri konusu, gerek çıkarılan yönetmelikler ile gerek ise Kurum tarafından verilen kararlar ile birlikte yeni yeni çerçevesini çizmektedir. Bu alanda faaliyet gösteren avukatlar hem kendini geliştirmeye açık olmalı, hem de temsil ve danışmanlık hizmeti verdikleri müvekkilleri ile konuya dair bilgi paylaşımında bulunulmalıdır. Bu kapsamda, kişisel verileri işlenen ilgili kişilere yönelik yazılı aydınlatma ve bilgilendirme metinleri hazırlanabilir, eğitim seminerleri yapılarak müvekkil ve bünyesindeki çalışanlara kişisel verilerin korunmasına dair bilgilendirme yapılabilir, şirket bünyesinde çalışan ve kişisel verilerin işlenmesi sürecinde aktif rol alan personel ile düzenli olarak bir araya gelinip şirketin veri politikasını ilgilendirebilecek kurul kararları ve mevzuat değişiklikleri ile ilgili paylaşımda bulunulabilir. Unutulmaması gerekir ki kişisel verilerin işlenmesi süreci kısa süreli değil sürekli devam eden ve güncelliğini koruması gereken bir projedir. Sürece dahil tüm paydaşların veri işletim sürecinden haberdar ve bilinçli olarak çalışmaları, yürütülen veri stratejisinin daha başarılı hayata geçirilmesine yardımcı olacaktır.

Advising Companies and Institutions on the Protection of Personal Data and Organizing Educational Programs

❑ Protection of personal data topic is still developing in our country. The personal data subject, which has been developing in our country in recent years, draws a new framework with both the regulations issued and the decisions made by the Authority. Lawyers operating in this field should be open to self-improvement and share information on the subject with their clients they provide representation and consultancy services. In this context, written clarification and informative texts can be prepared for the persons whose personal data are processed, training seminars can be held to inform the client and employees on the protection of personal data, regularly meet with the personnel working within the company and take an active role in the processing of personal data. Board decisions and legislative changes that may concern the policy can be shared. It should not be forgotten that the process of processing personal data is not a short-term project, but a continuous project that needs to be up-to-date. If all stakeholders involved in the process are aware of the data processing process and work consciously, it will help the data strategy to be implemented more successfully.

Şirketlere Veri Güvenliği İhlalleriyle Başa Çıkmak İçin Prosedür Geliştirilmesine Yardımcı Olunması

❑ Mevzuata uygun bir şekilde kişisel verileri işleyen ve bunları veri sisteminde depolayan veri sorumlusu, aynı zamanda bünyesindeki kişisel verilerin güvenliğinden de

Assisting the client in developing procedures to deal with data security breaches

❑ The data responsible will also be responsible for the security of personal data. In accordance with Article 12 of the Law, data responsible to prevent personal data from

sorumlu olacaktır. Kanunun 12. maddesinde veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu belirtilmiştir.

being processed illegally, to prevent personal data from being accessed illegally and to take all necessary technical and administrative measures to ensure the appropriate level of security to ensure the retention of personal data.

❑ Bu kapsamda veri sorumlularının, teknik ve hukuki destek ile güvenlik prosedürü geliştirmesi olası risklerin önüne geçilmesini sağlayabilecektir. İdari ve hukuki anlamda; mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları uygulanması ve kişisel verilerin mümkün olduğunca azaltılması gibi tedbirlere başvurulabilecektir. Teknik anlamda ise siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel verilerin bulutta depolanması gibi tedbirler alınarak kişisel verilerin korunması sağlanabilecektir.

❑ In this context, the development of security procedures with technical and legal assistance will prevent data risks from being prevented. It will be beneficial for the client to determine a procedure that is low cost, has high security in terms of data protection and complies with both national and international legislation.

Şirket Bünyesinde Verilerin Yurtdışına Aktarılması Konusunda Şirkete En Uygun Yöntemin Belirlenmesi

Evaluating the various mechanisms for the transfer of personal data outside the country and advising the client on the one that is appropriate for its particular circumstances

❑ Kişisel Verilerin Korunması Kanunu'nun 9.maddesinde kişisel verilerin yurtdışına aktarılması hususu düzenlenmiştir. Bu hükme göre verilerin yurtdışına aktarılabilmesi için ilgili kişinin açık rızası şart koşulmuştur. Ancak kanunun 5. ve 6. maddedeki şartları sağlanmakla birlikte, kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunması, yeterli koruma söz konusu değil ise Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın kişisel veriler yurt dışına aktarılabilecektir. Hangi ülkelerde yeterli korumanın bulunduğu Kişisel Verilerin Korunması Kurulu tarafından belirlenmektedir.

❑ The issue of transferring personal data abroad is regulated in Article 9 of the Personal Data Protection Law. According to this provision, the explicit consent of the person concerned is required in order to transfer the data abroad. However, while the law of the 5th and 6th conditions in the material provided, there is adequate protection in the country where transmission of personal data is not sufficient protection in question is an adequate protection of responsible data in Turkey and in the foreign countries to commit themselves in writing and the person concerned, subject to the approval of the Council open Personal data can be transferred abroad without seeking consent. In which countries there is sufficient protection, it is determined by the Personal Data Protection Board.

❑ Mevzuat hükümleri de göz önünde bulundurularak usule uygun bir şekilde verilerin yurtdışına aktarılması ve bir merkezde toplanması sağlanabilecektir. Burada en uygun yöntemin belirlenmesi için hukuki, teknik ve mali şartlar birlikte değerlendirilmelidir. Düşük maliyetli, verilerin korunması bakımından üst düzey güvenliğe sahip ve gerek ulusal gerek ise uluslararası mevzuata uygun bir prosedürün belirlenmesi müvekkil adına faydalı olacaktır.

❑ Considering the provisions of the legislation, it will be possible to transfer the data to abroad in accordance with the procedure and to collect them in a center. Here, the legal, technical and financial conditions should be evaluated together in order to determine the most appropriate method. It will be beneficial for the client to determine a procedure that is low cost, has high security in terms of data protection and complies with both national and international legislation.

Kişisel Verilerin Korunması Hukuku'nun ve KVK Avukatlığının Gelişimi

Development of Personal Data Protection Law and Advocacy

❑ Hayatın her alanında iç içe olduğumuz kişisel verilerin korunması hususu otuz yılı aşkın süredir Avrupa'da ayrı bir uzmanlık alanı olarak kendisini gösterirken, özellikle son beş yılda devasa boyutlara ulaşan elektronik ticarete dönüşüm sonrası dar bir niş alandan geniş bir çalışma alanına dönüşmüştür. Kişisel Verilerin Korunması

❑ While the issue of protecting personal data, which we are intertwined with in all areas of life, has shown itself as a separate area of expertise in Europe for more than thirty years, it has transformed from a narrow niche to a wide field of work after the transformation to electronic commerce, which has reached enormous dimensions in

Hukuku'na dair son yıllarda ülkemizde de yapılan çalışmalar ile birlikte AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile 28 Ocak 1981 tarihinde Strazburg'da imzalanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ile uyumlu, çağın gereklerine ayak uyduran 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili yönetmelikleri yürürlüğe girmiştir.

❑ Aynı zamanda Kişisel Verilerin Korunması Kurumu bünyesinde alınan kararlar neticesinde kişisel veri hukukuna ilişkin bir karar içtihatı da yavaş yavaş oluşmaktadır. Yakın zamana kadar bölgesel ve ulusal görülen kişisel verilerin işlenmesi hususu, yukarıda da belirttiğimiz gibi internetin ve elektronik ticaretin yaygınlaşmasıyla birlikte uluslararası bir hal almış; bu durum, Kişisel Verilerin Korunması Hukuku bağlamında avukatlar ve hukuk büroları tarafından yürütülen danışmanlık ve hizmet faaliyetlerini de ülke sınırlarının dışına çıkarmıştır. Bu durum avukatlara yeni bir uzmanlık alanı sağlamakla beraber birbirinden farklı birçok yargı bölgesinin kanunlarına aşina olma zaruretini de beraberinde getirmiştir. Bu noktada ilgili alanda çalışan avukatlara düşen temel görev, müvekkillerine kişisel veri işleme sürecinin hangi aşamasında olursa olsun ihtiyaç duyduğu hukuki ve teknik desteği en hızlı ve en pratik şekilde aktarmaktır.

❑ Yukarıda da belirttiğimiz gibi gerçek ve tüzel kişiler bakımından veri işleme prosedürleri kısa bir zaman dilimini değil, devinim gösteren uzun bir süreci gösterir şekilde karşımıza çıkmaktadır. Bu noktada doğru adımları atmak yalnızca bugünü kazanmaya yol açmayacak, aynı zamanda yarına yatırım yapıp veri işleme işlemlerinin sağlam bir zemine oturmasına yardımcı olacaktır.

the last five years. Along with the studies carried out in our country in recent years on the Law on the Protection of Personal Data, the EU Parliament and Council's European Union General Data Protection Regulation dated 27 April 2016 and numbered 2016/679 and "Personal Data No. Law No. 6698 on the Protection of Personal Data and its related regulations, which is compatible with the "Convention on the Protection of Individuals Against Automatic Processing", has come into force.

❑ At the same time, as a result of the decisions taken within the Personal Data Protection Authority, a decision case law on personal data law is gradually being formed. The issue of processing personal data, which was considered regional and national until recently, has become international with the widespread use of the internet and electronic commerce as mentioned above; This situation has also taken the consultancy and service activities carried out by lawyers and law offices outside the borders of the country in the context of Personal Data Protection Law. While this provides lawyers with a new field of expertise, it has brought the necessity of being familiar with the laws of many different jurisdictions. At this point, the main duty of lawyers working in the relevant field is to convey the legal and technical support they need to their clients in the fastest and most practical way, regardless of the stage of personal data processing.

❑ As mentioned above, data processing procedures for natural and legal persons are not a short period of time, but a long process. At this point, taking the right steps will not only lead to win today, but also help invest in tomorrow and put data processing operations on a solid ground.

Kişisel Verilerin Korunmasına Yönelik Türk Ceza Kanununda ve Kişisel Verilerin Korunması Kanununda Mevcut Yaptırımlar ile Bu Yaptırımlara Karşı Hukuki Çareler

Av.Muhittin Yoran

Türk Ceza Kanununda Yer Alan Kişisel Verilerin Korunmasına Yönelik Hükümler:

❑ Kişi mahremiyetinin ve özel hayatın korunması hakkının bir uzantısı olarak ***"kişisel verilerin korunması"*** hakkının ihlal edilmesi durumunda, failler hakkında getirilen cezai ve idari yaptırımlarla, söz konusu hakkın korunması amaçlanmıştır.

❑ Bu bağlamda; kişisel verilerin korunması amacıyla uygulama alanı bulan ceza hukuku yaptırımları olarak; 6698 sayılı Kişisel Verilerin Korunması Kanununun (KVKK) 17.maddesinin yaptığı atıfla 5237 sayılı Türk Ceza Kanunu'nun (TCK) ***"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"*** başlıklı Dokuzuncu Bölümünde yer alan;

→TCK-135 Md. ile ***"kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu",***

→TCK-136 Md. ile ***"kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu",***

→TCK-137 Md. ile bu iki suçun ***nitelikli halleri*** ve

→TCK-138 Md. ile ***"kişisel verileri yok etmeme suçu"*** düzenlenmiştir.

❑ TCK'nın bahsedilen bu madde hükümlerinde;

○ TCK-135.md.1.fıkrada, hukuka aykırı olarak kişisel verileri kaydeden kimseye ***bir yıldan üç yıla kadar hapis cezası*** verileceği, 2.fıkrada, bu kişisel verilerin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda verilecek ***cezanın yarı oranında artırılacağı***;

○ TCK-136.md.1.fıkrada kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, ***iki yıldan dört yıla kadar hapis cezası*** ile cezalandırılacağı, 2.fıkrada ise suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ***cezanın bir kat artırılacağı;***

Sanctions actuelles pour la protection des données personnelles dans le Code pénal turc et dans la loi sur la protection des données personnelles et recours juridiques contre ces sanctions

Dispositions relatives à la protection des données personnelles dans le Code pénal turc:

❑ C'est par les sanctions pénales et administratives imposées aux auteurs que l'on vise à protéger ***«le droit à la protection des données personnelles» e***n cas de violation de ce ***droit*** en tant que l'extension du droit à l'intimité et à la protection de la vie privée de la personne.

❑ Dans ce contexte; comme des sanctions pénales applicables à la protection des données personnelles; dans le chapitre IX du Code pénal turc (CPT) n° 5237, intitulée ***«crimes contre la vie privée et le secret de la vie»***, avec la référence de l'article 17 de la loi sur la protection des données personnelles (LPDP) n° 6698; dont les dispositions pertinentes sont ci-dessous;

→L'art. 135 du CPT, ***«Crime d'enregistrement illégal de données personnelles»,***

→L'art. 136 du CPT***,«Crime de transfert et de collecte illégale des données personnelles***»,

→L'art. 137 du CPT, ***«Cas qualifiés de ces deux crimes»,***

→L'art. 138 du CPT, ***«Crime de ne pas effacer les données personnelles».***

❑ En effet, dans des articles mentionnés du CPT, les dispositions suivantes s'appliquent:

○ Selon l'art.135-1 du CPT; la personne qui enregistre illégalement les données personnelles ***encourt une peine d'emprisonnement d'un à trois ans*** et selon l'art.135-2; si les données personnelles concernent les opinions politiques, philosophiques et religieuses des personnes et ses origines raciales; et les données personnelles obtenues illégalement, relatives aux tendances morales, à l'orientation sexuelle, à la santé ou à l'appartenance syndicale, ***la peine encourue est augmentée de moitié***.»

○ Selon l'art.136-1 du CPT; celui qui transfère illégalement les données personnelles à un tiers, et également celui qui les collecte et qui les diffuse ***encourt une peine d'emprisonnement comprise entre 2 ans et 4 ans*** et selon l'art.136-2 ; si la thématique du crime est des déclarations et des images enregistrées conformément aux cinquième et sixième alinéas de l'article 236 du Code de procédure pénale (CPP), la peine est doublée ».

o TCK-137.md'sinde, ***nitelikli haller*** olarak, bu suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi halinde, verilecek ***cezanın yarı oranında artırılacağı;***

o TCK-138.md'sinde de kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde ***1 yıldan 2 yıla kadar hapis cezası*** verileceği, ayrıca suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ***cezanın bir kat artırılacağı*** düzenlenmiştir.

❑ Yukarıdaki suçlara ilişkin uyuşmazlıklara; 5235 Sayılı Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev Ve Yetkileri Hakkında Kanunun 12.maddesi gereğince bu suçların cezalarının üst sınırının 10 yılı aşmadığı ve maddede düzenlenen katalog suçlar arasında olmadığı göz önünde bulundurulduğunda, (5271 Sayılı Ceza Muhakemesi Kanununun (CMK) yetki kurallarını düzenleyen 12.madde ve devamındaki hükümlere göre ***suçun işlendiği yerdeki***) ***Asliye Ceza Mahkemelerinde*** bakılması gerekmektedir.

❑ Genel bir düzenleme olan TCK-135,136 ve 138 maddelerde düzenlenen suçların tanımından ***herkes*** tarafından işlenebileceği, ancak ayrıca 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun (KVKK) 17.maddesinin TCK'ya atıf yapması nedeniyle, Veri İşleyen ve Veri Sorumlusu *(KVKK'nın tanımlar başlıklı 3.madde ğ) fıkrasında "**Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"** ve 3.madde ı) fıkrasında **"Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"** olarak tanımlanmıştır)* tanımlarına uyan gerçek ve tüzel kişilerinde suç faili olabilecekleri anlaşılmaktadır.

o Selon l'art.137 du CPT, comme ***des cas qualifiés*** (aggravant la peine); si les crimes aux articles précédents sont commises par un officier public abusant de l'autorité que lui confère l'exercice de ses fonctions ou en profitant des avantages liés à l'exercice d'une profession ou d'un commerce, ***la peine sera augmentée de moitié.***

o Selon l'art.138-1 du CPT; celui qui n'efface pas les données dans la durée déterminée par la loi, bien qu'il soit responsable de les effacer, ***encourt une peine d'emprisonnement allant d'un à deux ans.*** Et enfin, dans la deuxieme alinéa «si la thématique du crime est une donnée à effacer ou à supprimer selon le Code de procédure pénale (CPP), ***la peine est doublée***.

❑ ***Les Tribunaux correctionnels*** (du lieu où le crime est commis selon l'article 12 et suivants du Code de procédure pénale (CPP), qui définit la compétence territoriale des tribunaux) sont pour juger les crimes précédents, selon l'article 12 de la loi relative aux organisations, fonctions et compétences des tribunaux de première instance de juridiction judiciaire et des cours d'appel régionaux n° 5235, en considérant que les crimes mentionnés ne dépassent pas la durée d'emprisonnement de 10 ans de maximum et qu'ils ne sont pas dans la liste de crime de l'article.

❑ On considère par définition que les crimes dans les articles 135, 136 et 138 du CPT étant une loi générale, pourraient être commis par toutes les personnes. Cependant, en raison de référence de l'article 17 de la loi sur la protection des données personnelles (LPDP) au CPT, le responsable du traitement des données et le sous-traitant des données peuvent etre l'auteur du crime. (*Dans l'alinéa ğ) de l'art.3 du LPDP «**le sous-traitant est la personne physique ou morale qui traite les données personnelles uniquement pour le compte du responsable du traitement et qui base sur son autorisation de celui-ci**», et dans l'alinéa ı) du meme article«**le responsable du traitement des données person nelles est la personne physique ou morale qui détermine les finalités et les moyens de ces données personnelles et qui est responsable de la mise en place et de la direction du système d'enregistrement**».)*

❑ Tüzel kişilerin ceza sorumluluğu TCK-20.maddede ve tüzel kişiler hakkında uygulanacak cezalar TCK-60.maddelerde düzenlenmiş olup, bu suçların karşılığı olarak öngörülen hapis cezaları, TCK-20.md.1.fıkradaki ceza sorumluluğunun şahsiliği ilkesi sebebiyle sadece gerçek kişilere uygulanabilen yaptırım türlerinden biridir. Bu cezaların tüzel kişilere uygulama alanı bulunmadığından tüzel kişiler tarafından bu suçların işlenmesi halinde:(1) *Tüzel kişiliğin organlarının veya temsile yetkili gerçek kişilerin cezai sorumluluğunun doğması* ve (2) TCK-20.md.2.fıkradaki "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır." hükmü doğrultusunda *güvenlik tedbirlerinin uygulanabilmesi* mümkün olabilecektir.

❑ Tüzel Kişilerin bu fiilleri işlemeleri halinde haklarında TCK-60 maddede yer alan *(Faaliyet İzninin İptali, Eşya Müsaderesi ve Kazanç Müsaderesi)* güvenlik tedbirlerine hükmedilebilmesi için, suçu düzenleyen TCK'da veya özel kanunda bunun özel olarak belirtilmesi gerekmektedir (TCK-m.60/f4). Bu durumda TCK-140 maddede yer alan ***"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."***hükmü doğrultusunda Veri Sorumlusu ya da Veri İşleyen sıfatı taşıyan Tüzel Kişilerin bu fiilleri işlemeleri halinde:(1) Tüzel Kişiliğin organlarının veya temsile yetkili gerçek kişilerin cezai sorumluluğunun doğması ve aynı anda (2) Suçun tüzel kişinin yararına işlenmesi halinde Tüzel Kişilik hakkında güvenlik tedbirlerine hükmedilmesi mümkün olabilecektir.

❑ Bir diğer önemli husus ise bir fiilin hem bir suç hem de bir kabahat teşkil etmesi durumunda nasıl hareket edileceğine ilişkindir. Bu Konuya 5326 sayılı Kabahatler Kanunun 15.maddesi 3.fıkrasında getirilen **"Bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Ancak, suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanır."** hükmü ile Ceza Hukukundaki aynı fiil nedeniyle sanığın ancak bir defa yargılanabilmesi ve bir defa cezalandırılabilmesini ifade eden Ne Bis İn İdem İlkesi'ne uyumlu bir çözüm getirilmiştir.

❑ Türk Ceza Kanununda zamanaşımı, dava ve ceza zamanaşımı olmak üzere iki şekilde düzenlenmiş olup, zamanaşımı süresinin geçmesi ile devletin cezalandırma yetkisi ortadan kalkmaktadır. Dava zamanaşımı süresinin geçmesi halinde bu durum, kamu davasının açılmasına veya bakılmakta olan bir davanın devam edilmesine engel olmakta; ceza zamanaşımı süresinin geçmesi ile ise, kesinleşmiş olan mahkûmiyet hükmünün infazına başlanması engellenmektedir.

❑ La responsabilité pénale des personnes morales est réglementée dans l'article 20 du CPT et les peines prévues sont dans l'article 60 du CPT. Les peines d'emprisonnement prévues pour ces crimes sont l'un des types de sanctions qui ne peuvent être appliquées qu'à des personnes physiques, à cause de la principe de responsabilité personnelle selon l'alinéa I de l'article 20 du CPT. Étant donné que ces sanctions ne sont pas applicables aux personnes morales, au cas où ces crimes seraient commis par des personnes morales: 1) il est possible que la responsabilité pénale des organes ou des représentants des personnes morales soit engagée et 2) il sera applicable des dispositions et des mesures de sécurité spécifiques pour des personnes morales, selon l'alinéa II de l'article 20 du CPT.

❑ Dans le cas où les personnes morales commettent ces crimes, pour les condamner à des mesures de sécurité spécifiques (annulation d'autorisation d'exploitation, confiscation des biens, confiscation du gain) à l'art.60 du CPT, il faut qu'il soit prévu et prononcé par CPT ou une autre loi spéciale qui réglemente le crime. Puisque selon la disposition de l'art.140 du CPT **«si des personnes morales commettent des crimes des articles précédents, par conséquent, on peut prononcer des mesures de sécurité spécifiques pour eux»** ainsi le responsable du traitement des données et le sous-traitant des données commettent ces crimes, il sera possible:1)*la responsabilité pénale des organes ou des représentants des personnes morales soit engagé et en meme temps, 2)si le crime est commis au profit de la personne morale, condamner* à des mesures de sécurité spécifiques.

❑Une autre question importante est de comment trouver une solution, si un acte constitue à la fois un crime et un délit. Cette question est résolue à l'aide de la disposition l'article 15 de la loi sur les délits n° 5326 ***«si un acte est défini à la fois comme un délit et un crime, des sanctions ne peuvent être imposées que pour le crime. Cependant, dans les cas où des sanctions ne peuvent plus être appliquées en raison du crime, des sanctions sont appliquées en raison d'un délit ».*** C'est une solution conforme au principe ***Ne Bis In Idem***, qui stipule que l'accusé ne peut être jugé et puni qu'une seule fois en raison du même acte dans le droit pénal.

❑ Le délai de prescription est réglementé par CPT de deux manières: la prescription de poursuite et la prescription de peine, et l'expiration du délai de prescription sera la cause d'abandonnement du pouvoir de punir de l'État. En cas d'expiration du délai de prescription de poursuite, cela empêche la mise en mouvement de l'action publique ou la poursuite d'une affaire; mais avec l'expiration du délai de prescription de peine empêche de commencer à l'exécution de la peine finale.

❑ Dava zamanaşımı süresi, her suç için Kanunda ayrı ayrı öngörülen cezanın üst sınırı dikkate alınarak ve TCK-66.md.1.fıkradaki ayrımlara göre belirlenir. TCK-135, 136 ve 138.maddelerde düzenlenen kişisel veriler aleyhindeki bu suçlarda öngörülen cezaların üst sınırı beş yılı aşmamakta olduğundan ve bu durum TCK-66.md.1.fıkra e)bendindeki "Beş yıldan fazla olmamak üzere hapis veya adlî para cezasını gerektiren suçlarda sekiz yıl" ibaresine uyduğundan ***dava zamanaşımı süresi sekiz yıldır. Ceza zaman aşımı süresi ise TCK-68.Md.1.fıkra e) bendine göre 10 yıldır.***

❑ TCK-135, 136 ve 138.maddelerde düzenlenen kişisel veriler aleyhindeki bu suçlarda da, CMK-102.md.de yer alan koşulların gerçekleşmesi halinde Hakim şüpheli veya sanıklar hakkında tutukluluğa hükmedebilir. ***Tutukluluk süresi***; CMK-102.md.1.fıkradaki "Ağır ceza mahkemesinin görevine girmeyen işlerde tutukluluk süresi en çok bir yıldır. Ancak bu süre, zorunlu hallerde gerekçeleri gösterilerek altı ay daha uzatılabilir." hükmü gereğince ***en çok bir yıla kadar, zorunlu hallerde bir yıl altı aya kadar uzatılabilir.***

❑ Kişisel verilerin kaydedilmesi, kişisel verileri hukuka aykırı olarak verme veya ele geçirme ve kişisel verileri yok etmeme suçlarının soruşturulması ve kovuşturulması şikâyete bağlı değildir. (TCK-139.md.)

❑ Yargılama sonucunda, bu suçların karşılığı olarak ***bir yıl veya daha az süreli hapis cezasına*** (kısa süreli hapis cezası) (TCK-49.md.) hükmedilmesi halinde ve TCK'da yazan şartlar mevcutsa Hâkim, bu cezaları ***adli para cezası*** da dâhil olmak üzere ***seçenek yaptırımlara*** çevirebilir.(TCK- 50.md.)

❑ Yargılama sonucunda, bu suçların karşılığı olarak **iki yıl veya daha az süreli hapis cezası veya adlî para cezasına** hükmedilmesi halinde ve CMK-231.md.6.fıkrada yazan şartlar oluşmuşsa Hâkim, kurulan hükmün sanık hakkında bir hukukî sonuç doğurmayacağını ifade eden Hükmün Açıklanmasının Geri Bırakılması ***(HAGB) Kararı*** verebilir.

❑ Bu suçların işlenmesi sonucu Asliye Ceza Mahkemelerince hükmedilen cezalara karşı CMK-272-285.md.de yer alan İstinaf ve CMK-286-307.md.de yer alan ve Temyiz hükümlerine göre olağan kanun yoluna başvurulabilir. Asliye Mahkemesince verilen bahse konu hüküm hürriyeti bağlayıcı bir ceza ise, hükmün açıklanmasından itibaren **7 gün içinde** istinaf başvurusu yapılabilir(CMK-273.md). Bu suçlarda sadece hapis cezasından çevrilen adlî para cezaları söz konusu olabildiğinden ve bunlarda (CMK-272.madde 3.fıkra a) bendi gereğince) istinaf kapsamı dışında kaldığından, adli para cezalarına karşı istinaf yoluna başvurulamayacaktır.

❑ İl se détermine le délai de prescription de porsuite en considérant les maximums des peines prévues au CPT pour chacun des crimes et aussi les distinctions dans l'article 66-I du CPT. ***Le délai de prescription de poursuite*** des crimes contre les données personnelles qui se prescrivent dans les articles 135, 136 et 138 du CPT ***c'est huit ans***, puisque les maximums des peines prévues en matière de ces crimes ne dépassent pas cinq ans étant en accord avec la disposition de l'alinéa I.e) de l'article 66 du CPT. ***Le délai de prescription de peine c'est dix ans*** selon l'alinéa I.e) de l'article 68 du CPT.

❑ Dans ces crimes contre les données personnelles réglementés dans les articles 135, 136 et 138 du CPT le juge peut ordonner le suspect ou l'accusé en détention si les conditions de détention mentionnées de l'article 102 du CPP sont remplies. Selon l'article 102-I du CPP «Pour les affaires qui ne relèvent pas de la compétence de Cour d'assises, la durée maximale de la détention est d'un an. Toutefois, cette période peut être prolongée de six mois supplémentaires en indiquant les raisons dans les cas obligatoires» ***la période de détention de ces crimes peut être prolongé jusqu'à un an maximum et dans des cas obligatoires jusqu'à un an et six mois.***

❑ L'enquête et la poursuite de ces crimes «d'enregistrement illégal de données personnelles, de transfert et de collecte illégale des données personnelles, de ne pas effacer les données personnelles» ne requiert pas l'objet d'une plainte. (L'Art.139 du CPT)

❑ À la suite du procès de jugement contre ces crimes, si le juge prononce une peine d'emprisonnement ***d'un an ou de moins*** (la peine d'emprisonnement de courte durée) (L'Art.49 du CPT) et que les conditions spécifiées au CPT sont disponibles, le juge peut convertir ces peines en ***sanctions alternatives***, y compris des ***amendes judiciaires*** (L'Art.50 du CPT)

❑ À la suite du procès de jugement contre ces crimes, si le juge prononce une peine d'emprisonnement ***de deux ans ou de moins ou des amendes judiciaires*** et que les conditions spécifiées à l'article 231-VI du CPP sont disponibles, le juge peut décider à un ***report de l'annonce du verdict*** qui affirme que le verdict n'a aucun effet juridique sur l'accusé.

❑ Les voies de recours ordinaires peuvent être appliquées contre les verdicts prononcés par les tribunaux correctionnels soit devant la cour d'appel régional selon les dispositions des articles de 272 à 285 du CPP ou soit devant la cour de cassation selon les dispositions des articles de 286 à 307 du CPP. Si le verdict prononcé par le tribunal correctionnel se préoccupe des sanctions restreignant la liberté un recours peut être formé ***dans les 7 jours*** à compter de l'annonce du verdict (Art.273 du CPP). Les amendes judiciaires infligées pour ces crimes ne peuvent faire l'objet d'un appel (Art.273-3 du CPP).

❑ İstinaf Talebi üzerine yapılan yargılama sonucunda Bölge Adliye Mahkemesi (İstinaf Mahkemesi) tarafından; 1) istinaf başvurusunun esastan reddi, 2) hukuka aykırılığın düzeltilerek istinaf başvurusunun esastan reddi, 3) hükmün bozulması ve dosyanın yeniden incelenmek ve hükmolunmak üzere hükmü bozulan ilk derece mahkemesine veya kendi yargı çevresinde uygun göreceği diğer bir ilk derece mahkemesine gönderilmesi 4) ilk derece mahkemesinin hükmünün kaldırılarak mahkûmiyet veya beraat kararları verilebilir.

❑ Bölge Adliye Mahkemelerinin bozma dışındaki kararları temyize götürülebilir. Ancak, hükmedilen cezanın miktarı ve suç türü bakımından bazı istinaf mahkemesi kararları aleyhine temyiz kanun yolu kapatılmıştır. Örneğin TCK-135,136,137 ve 138. Maddede yer alan ve incelememize konu suçlardan ötürü, Asliye Ceza Mahkemesinde verilen beş yıl veya daha az hapis cezaları ile miktarı ne olursa olsun adlî para cezalarına karşı istinaf başvurusunun esastan reddine dair bölge adliye mahkemesi kararları aleyhine CMK-286.madde, 2.fıkra a) bendi gereğince temyiz kanun yoluna başvurulamayacaktır. Temyiz yolu kapalı olan diğer kararlar CMK-286.maddenin diğer fıkralarında sayılmıştır. Temyiz istemi, hükmün açıklanmasından itibaren on beş gün içinde yapılabilir(CMK-291.madde).

❑ Uzlaştırma kapsamında olan suçlar, kural olarak soruşturulması ve kovuşturulması şikâyete tabi suçlar olduğundan; bu nitelikte olmayan bu suçlar; faili bakımından TCK-253.madde 1.fıkra c)fıkrasındaki "Mağdurun veya suçtan zarar görenin gerçek veya özel hukuk tüzel kişisi olması koşuluyla, ***suça sürüklenen çocuklar*** bakımından ayrıca, üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar." istisna hükmü hariç olmak üzere, TCK-253 ila 255.madde arasında düzenlenen ***"Uzlaştırma"*** hükümlerine tabi değildir.

❑ TCK'nın Nitelikli Haller başlıklı 137.Md.1.fıkrasında; ***"kişisel verilerin hukuka aykırı olarak kaydedilmesi (TCK-135.md.)"*** ve ***"kişisel verileri hukuka aykırı olarak verme veya ele geçirme (TCK-136.md.)"*** suçlarının; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi halinde öngörülen cezanın yarı oranında artırılacağı belirtilmiştir. ***"Kişisel verileri yok etmeme (TCK-138.md.)"*** suçu ise nitelikli haller kapsamı dışında bırakılmıştır. Bunun yanında, ***Disiplin Hukukundaki disiplin soruşturmasının adli soruşturma veya kovuşturmadan bağımsızlığı ilkesi*** çerçevesinde, kişisel verilerin korunmasında caydırıcı etkiyi artırmak amacıyla, örneğin kolluk görevlilerinin disiplin hükümlerini düzenleyen 7068 Sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanunun 8.md.6.fıkra z), aa) ve bb) bentlerinde üç ayrı disiplinsizlik fiili düzenlenerek, bu fiillerin kolluk görevlisi tarafından işlenmesi halinde ayrıca ***meslekten çıkarma cezası*** verilmesi öngörülmüştür.

❑ Les décisions suivantes peuvent être prises par la cour d'appel régionale à la suite du jugement sur le rocours d'appel: 1) Refus de la demande d'appel sur le fond, 2) Refus de la demande d'appel sur le fond en corrigeant l'illégalité, 3) Rejet le verdict et renvoyer le dossier afin de réexaminer et rejuger au tribunal de première instance ou à un autre tribunal de première instance dans sa propre juridiction, 4) Condamnation ou acquittement en annulant le verdict de tribunal de première instance.

❑ Les décisions des cours d'appel régionaux sont susceptibles de voie de cassation sauf celles de rejet de verdict. Cependant, les recours de cassation sont fermés contre certaines décisions de la cour d'appel, en ce qui concerne le montant de la peine et le type de crime. Par exemple, en raison des crimes dans les articles 135-138 du CPT, un recours de cassation ne peut être introduit selon l'alinéa II.a de l'article 286 du CPP; à l'opposition des peines de cinq ans ou de moins devant le tribunal correctionnel et des décisions de la cour d'appel régionale concernant le refus de la demande d'appel sur le fond contre les amendes judiciaires quel qu'en soit le montant. Le recours de cassation peut être faite dans les quinze jours suivant l'annonce du verdict (Art.291 du CPP).

❑ Les enquête et les poursuites des crimes couvertes par la médiation pénale, dépendent des plaintes comme une règle générale. Ces crimes n'étant pas de cette nature, ils ne sont pas susceptibles de dispositions de ***«La médiation pénale»*** réglementées dans les articles 253 et 255 du CPT, à l'exception de la disposition de l'article 253-I.c du CPT ***«Crimes nécessitant une peine d'emprisonnement dont la limite maximum n'est pas supérieure à trois ans ou une amende judiciaire, en ce qui concerne les enfants, à condition que la victime soit une personne physique ou une personne morale de droit privé. »***

❑ Il est spécifié dans l'alinéa I de l'article 137 du CPT, comme des cas qualifiés : ***« des crimes d'enregistrement illégal de données personnelles. (Art.135 du CPT)»*** et ***«des crimes de transfert et de collecte illégale des données personnelles. (Art.136 du CPT)»*** que les crimes définis seront augmentés de moitié dans le cas où ses auteurs seraient des officiers publics abusant de l'autorité que leur confère l'exercice de ses fonctions ou profitent des avantages liés à l'exercice d'une profession ou d'un commerce. Cependant ***« le crime de ne pas effacer les données personnelles. (Art.138 du CPT)»*** est exclu du champ des cas qualifiés. D'autre part, dans le cadre du ***«principe d'indépendance de l'enquête disciplinaire; à des enquêtes judiciaires ou à des poursuites»*** en droit disciplinaire, afin d'augmenter l'effet dissuasif dans la protection des données personnelles, par exemple, trois actes d'indiscipline distincts sont imposés par l'article 8-VI de la loi sur les dispositions disciplinaires de la police n° 7068 et lorsque ces actes sont commis par des agents de la police, une sanction disciplinaire ***«licenciement de l'agent»*** est également prévue.

Kişisel Verilerin Korunması Bağlamında İdari Para Cezaları:

❑ İncelememizin asıl konusunu oluşturan Kişisel Verilerin Korunması Kapsamında Uygulanan İdari Yaptırımlar ise 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve 5326 sayılı Kabahatler Kanununda ele alınmıştır.

❑ 6698 sayılı KVKK-18.md'de Kabahatler başlığı altında idari yaptırımlar düzenlenmiştir. Bu başlıkta sayılan hususlara aykırı davranan gerçek veya tüzel kişi veri sorumlularına 6698 sayılı KVKK-22/ğ.md. ile verilen yetki gereğince Kişisel Verileri Koruma Kurulunca idari para cezası verilmesi öngörülmüştür. Buna göre;

○ Aydınlatma yükümlülüğünü yerine getirmeyenler için 5.000 TL'den- 100.000 TL'ye kadar (2020 yılı yeniden değerleme oranına göre: 9.012 TL'den- 180.263 TL'ye kadar) (KVKK-md.18/1-a),

○ Veri güvenliğine ilişkin gerekli tedbirleri almayanlar için 15.000 TL'den- 1.000.000 TL'ye kadar (2020 yılı yeniden değerleme oranına göre: 27.031 TL'den- 1.802.640 TL'ye kadar) (KVKK-md.18/1-b),

○ Kişisel Verileri Koruma Kurulu tarafından alınan kararların gereğini yapmayanlar için 25.000 TL'den- 1.000.000 TL'ye kadar (2020 yılı yeniden değerleme oranına göre:45.062 TL'den- 1.802.640 TL'ye kadar) (KVKK-md.18/1-c),

○ Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler için de 20.000 TL'den-1.000.000 TL'ye kadar (2020 yılı yeniden değerleme oranına göre:36.050 TL'den- 1.802.640 TL'ye kadar) (KVKK-md. 18/1-ç) idari para cezaları verilmektedir.

İdari Para Cezalarının Yargısal Denetimi:

İdari Para Cezalarının Yargısal Denetiminde Görevli Yargı Yeri ve Mahkeme:

❑ Bağımsız düzenleyici bir idari organ olarak Kişisel Verileri Koruma Kurulunca verilen idari para cezalarının Anayasa'nın 125. maddesinin birinci fıkrasında yer alan ***"İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır."*** ilkesi gereğince yargı denetimine tabi olacağı konusunda kuşku olmamakla birlikte, bu denetimin idari yargı yerlerinde mi, yoksa adli yargı yerlerinde mi yapılacağı konusu hukukumuzdaki en tartışmalı konulardan biri olmuştur.

Amendes administratives dans le contexte de la protection des données personnelles

❑ Le sujet principal de ce texte, les sanctions administratives imposées dans le cadre de la protection des données personnelles sont traitées dans la loi sur la protection des données personnelles (LPDP) n° 6698 et la loi sur les délits n° 5326.

❑ Les sanctions administratives sont réglementées sous la rubrique «des délits» dans l'article 18 du LPDP, n° 6698. Il est précisé qu'une amende administrative sera infligée pour des responsables du traitement soit des personnes physiques ou morales qui agissent contre aux dispositions dans ce titre, par le comité de protection des données personnelles (CPDP) conformément à l'autorisation accordée par l'article 22.ğ du LPDP, n° 6698. Les amendes administratives en question sont:

○ Pour ceux qui ne remplissent pas l'obligation d'éclairage, de 5.000 ₺ à 100.000 ₺ (selon le taux de réévaluation de 2020: de 9.012 ₺ à 180.263 ₺) (Art.18/1-a du CPDP),

○ Pour ceux qui ne prennent pas les mesures nécessaires en matière de sécurité des données, de 15.000 ₺ à 1.000.000 ₺ (selon le taux de réévaluation de 2020: de 27.031 ₺ à 1.802.640 ₺) (Art.18/1-b du CPDP),

○ Pour ceux qui ne se conforment pas aux décisions prises par le CPDP, de 25.000 ₺ à 1.000.000 ₺ (selon le taux de réévaluation de 2020: de 45.062 ₺ à 1.802.640 ₺) (Art.18/1-c du CPDP),

○ Pour ceux qui agissent contre l'obligation d'enregistrements au système d'enregistrement pour des responsables du traitement et contre l'obligation de notification, de 20.000 ₺ à 1.000.000 ₺ (selon le taux de réévaluation pour 2020: de 36.050 ₺ à 1.802.640 ₺) (Art.18/1-ç du CPDP),

Les voies de recours contre les amendes administratives

l'Ordre de juridiction et le Tribunal en charge au contrôle juridictionnelle des amendes administratives

❑ Il n'y a aucun doute qu'ils seront soumis à un contrôle juridictionnel des amendes administratives infligées par le comité de protection des données personnelles (CPDP), en tant qu'une autorité administrative indépendante et regulative, selon l'alinéa I de l'article 125 de la Constitution ***«tous les actes et décisions de l'administration peuvent faire l'objet d'un recours judiciaire»***. Cependant, la question de savoir si ce contrôle sera exercé devant l'ordre judicaire ou administratif a été l'une des questions la plus controversée de droit turc.

❑ Mevcut hukuk sistemimizde idari yaptırımların yargısal denetimlerinin nasıl yapılacağı; idari yaptırım içeren kanunlar için genel kanun mahiyetini koruyan 5326 sayılı Kabahatler Kanununun aşağıda belirtilen 3.madddesi hükmü ile şu şekilde düzenlenmiştir:

> ***"Genel kanun niteliği***
> ***Madde 3- (Değişik: 6/12/2006-5560/31 md.) (1) Bu Kanunun; a) İdarî yaptırım kararlarına karşı kanun yoluna ilişkin hükümleri, diğer kanunlarda aksine hüküm bulunmaması halinde, b) Diğer genel hükümleri, idarî para cezası veya mülkiyetin kamuya geçirilmesi yaptırımını gerektiren bütün fiiller hakkında, uygulanır"***

❑ O halde, görevli yargı yerini belirlemede ana kıstas, bu hüküm gereğince; idarenin idari para cezası için dayanak aldığı kanunda yargı denetimine ilişkin bir hüküm olup olmadığına bakarak belirlenebilecektir. Eğer yargı denetimine ilişkin söz konusu kanunda bahsedilen idari yaptırımların idari yargı yerlerinde denetleneceğine ilişkin özel bir hüküm bulunmuyorsa, bu denetimin adli yargıda ve 5326 sayılı Kabahatler Kanunda belirtilen usul ve esaslara göre yapılması gerekmektedir.

❑ 6698 sayılı KVKK hükümleri bu doğrultuda incelendiğinde, idari yaptırımların yargısal denetimine yani kanun yoluna özel bir hüküm sevk edilmediğini, bu sebeple de idari yaptırımların yargısal denetiminin 5326 sayılı Kabahatler Kanununun 27.maddesine göre ***adli yargı yolu ile (sulh ceza hakimlikleri)*** yapılacağı açıktır.

❑ Haksız ve hukuka aykırı olarak Kişisel Verileri Koruma Kurulu tarafından verilmiş idari para ceza kararlarına karşı Kabahatler Kanunu'nun 27. maddesinde "***Başvuru Yolu" adı verilen adli yargılama usulü getirilerek,*** sulh ceza mahkemeleri (5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanuna eklenen Ek Madde-1 ile sulh ceza mahkemesine yapılan atıflar sulh ceza hâkimine yapılmış sayıldığından ***sulh ceza hakimlikleri***) ***maddi hukuk ve usul hukuku yönünden*** yargı denetimini yapmakla görevli kılınmıştır.

❑ Başvuru yolu; Cumhuriyet savcısının katılımının olmaması sebebiyle ceza muhakemesi bakımından yürürlükten kaldırılan 1412 sayılı Ceza Muhakemeleri Usul Kanununda yer alan ***şahsi davaya***, muhatabın İdare olması ve işlemin idari karar olması sebebiyle de ***iptal davasına*** benzetilebilecek, bir hak arama yöntemi olarak düzenlenmiştir.

❑ Ancak; Kabahatler Kanununun 27.md.8.fıkrasındaki ***"İdarî yaptırım kararının verildiği işlem kapsamında aynı kişi ile ilgili olarak idarî yargının görev alanına giren kararların da verilmiş olması halinde; idarî yaptırım kararına ilişkin hukuka aykırılık iddiaları bu***

❑ En droit turc, Il est indiqué comment faire des controls juridictionnels contre des amendes administratives, avec la disposition ci-dessous de l'article 3 de la loi n° 5326 sur les délits qui préserve son caractère général pour les lois contenant des sanctions administratives:

> ***«Son caractère général***
> ***Article 3-a) les dispositions de la présent loi concernant la voie de recours contre les décisions de sanction administrative sont appliquées en l'absence de dispositions contraires dans d'autres lois. b) les autres dispositions générales de la présente loi s'appliquent à tous les actes exigeant des amendes administratives ou des sanctions pour transfert de propriété au public.»***

❑ Par conséquent, conformément à cette disposition; le principal critère pour déterminer la juridiction compétente, il faut comprendre s'il existe une disposition relative au contrôle **juridictionnelle** dans la loi sur laquelle l'administration est le fondement de l'amende administrative. S'il n'existe pas une disposition particulière prévoyant que les amendes administratives mentionnées dans la loi seront contrôlées devant l'ordre administratif, ce contrôle doit être effectué devant l'ordre judiciaire conformément aux principes et procédures spécifiés dans la loi sur les délits n° 5326.

❑ Lorsque les dispositions du LPDP, n° 6698 sont examinées dans ce sens, İl est précis qu'aucune disposition spéciale n'a été imposée sur le contrôle juridictionnel des sanctions administratives, c'est-à-dire sur les voies de recours, et que, pour cette raison, des sanctions administratives seront contrôlées devant l'ordre judiciaire (juge pénale de paix) conformément à l'article 27 de la loi sur les délits n° 5326.

❑ Dans ce contexte, les juges pénaux de paix ont été chargés du contrôle judiciaire en termes de droit matériel et de droit procédural contre les amendes administratives prononcées injustement et illégalement par le comité de protection des données personnelles, en introduisant la procédure judiciaire appelée ***"la voie d'application"*** à l'article 27 de la loi sur les délits.

❑ ***La Voie d'application*** est réglementée comme une méthode de recours qui peut être comparée soit en matière de procédure pénale, à ***l'affaire personnelle*** en raison de l'absence de participation du procureur de la République selon les dispositions du Code abrogée de procédure pénale n° 1412, soit à ***l'affaire d'annulation*** puisque le destinataire est l'administration et qu'il s'agit une décision administrative.

❑ Cependant; une exception à cette règle générale a été apportée avec la disposition de l'alinéa 8 de l'article 27 de la loi sur les délits ***«dans le cas où des décisions relevant de la compétence de la justice administrative concernant la même personne entrent également dans le cadre de la***

işlemin iptali talebiyle birlikte idarî yargı merciinde görülür" hükmüyle bu genel kurala bir istisna getirilmiş olup, 27.maddenin diğer hükümleri de şu şekildedir:

"Başvuru yolu
Madde 27- (1) İdarî para cezası ve mülkiyetin kamuya geçirilmesine ilişkin idarî yaptırım kararına karşı, kararın tebliği veya tefhimi tarihinden itibaren en geç onbeş gün içinde, sulh ceza mahkemesine (sulh ceza hakimliğine) başvurulabilir. Bu süre içinde başvurunun yapılmamış olması halinde idarî yaptırım kararı kesinleşir.

(2) Mücbir sebebin varlığı dolayısıyla bu sürenin geçirilmiş olması halinde bu sebebin ortadan kalktığı tarihten itibaren en geç yedi gün içinde karara karşı başvuruda bulunulabilir. Bu başvuru, kararın kesinleşmesini engellemez; ancak, mahkeme (sulh ceza hakimliği) yerine getirmeyi durdurabilir.

(3) Başvuru, bizzat kanunî temsilci veya avukat tarafından sulh ceza mahkemesine (sulh ceza hakimliğine) verilecek bir dilekçe ile yapılır. Başvuru dilekçesi, iki nüsha olarak verilir.

(4) Başvuru dilekçesinde, idarî yaptırım kararına ilişkin bilgiler, bu karara karşı ileri sürülen deliller açık bir şekilde gösterilir. Dilekçede ayrıca, başvurunun süresinde yapılmasını engelleyen mücbir sebep dayanaklarıyla gösterilir.

(5) İdarî yaptırım kararının mahkeme tarafından verilmesi halinde, bu karara karşı ancak itiraz yoluna gidilebilir.

(6) Soruşturma konusu fiilin suç değil de kabahat oluşturduğu gerekçesiyle idarî yaptırım kararı verilmesi halinde; kovuşturmaya yer olmadığı kararına itiraz edildiği takdirde, idarî yaptırım kararına karşı başvuru da bu itiraz merciinde incelenir.

(7) Kovuşturma konusu fiilin suç değil de kabahat oluşturduğu gerekçesiyle idarî yaptırım kararı verilmesi halinde; fiilin suç oluşturmaması nedeniyle verilen beraat kararına karşı kanun yoluna gidildiği takdirde, idarî yaptırım kararına karşı itiraz da bu kanun yolu merciinde incelenir.

transaction déjà prise concernant la décision de sanction administrative; les allégations d'illégalité relative à la décision de sanction administrative sont jugées devant la juridiction administrative avec la demande d'annulation de cette transaction». Les autres dispositons sont tel que:

la Voie d'application
Article 27-(1)Un recours contre l'amende administrative et de la décision de sanction administrative concernant le transfert de propriété au public peut être introduit devant le juge pénal de paix dans un délai de quinze jours au plus tard à compter de la notification ou prononciation de la décision. Si le recours n'est pas introduit dans ce délai, la décision de sanction administrative devient définitive.

(2) Lorsque le délai de recours contentieux est dépassé en raison de l'existence d'un cas de force majeure, un recours contre la décision en question peut être formé dans un délai de sept jours au plus tard à compter de la date à laquelle ce motif est éliminé. Ce recours n'empêche pas la décision d'être definitive; cependant, le juge pénal de paix peut arrêter l'exécution.

(3) le Recours est soumis au juge pénal de paix personnellement ou par le représentant légal ou l'avocat accompagné d'une requête. La requête doit être présentée en deux exemplaires.

(4) Dans la requête de recours sont présentées évidemment les informations relatives à la décision de sanction administrative et les preuves concrètes suggérées contre cette décision. la Requête est également indiquée avec des motifs de force majeure qui empêchent la demande d'être faites à temps.

(5) Si la décision de sanction administrative est prise par le tribunal, seul un recours appelé «Objection» peut être formé contre cette décision.

(6) Lorsqu'une décision de sanction administrative est prise à cause de l'acte faisant l'objet d'une enquête n'est pas un crime mais un délit; et si une objection est formulée contre «le classement sans suite», la requête d'objection contre la décision de sanction administrative est examinée également devant le juge traitant de l'objection.

(7) Lorsqu'une décision de sanction administrative est prise à cause de l'acte faisant l'objet d'une poursuite n'est pas un crime mais un délit; et si un recours est formulé contre «la décision d'acquittement étant donné que l'acte ne constituait pas un crime», la requête contre la décision de sanction administrative est examinée également devant la cour de voie de recours.

❑ Burada dikkat edilmesi gereken noktalardan en önemlisi; denetimin idari yargı yerlerinde yapılması durumunda; idari para cezasının iptali davasındaki idari işlem teorisine uygun bir şekilde, idari işlemin unsurları bakımından ve usul bakımından idari yargılama hukuku usul ve kurallarına göre denetimin yapılması gerekiyorken, 5326 sayılı Kabahatler Kanununun getirdiği sistemin idari bir işlemin ötesinde, ceza hukuku ve ceza muhakemeleri hukukunun genel prensipleriyle ve usul kurallarıyla yakın ilişki içinde olduğu gerçeğidir. Nitekim, Kabahatler Kanununda, kanunilik, zaman ve yer bakımından uygulama, sorumluluğun esasları, hukuka uygunluk nedenleri ile kusurluluğu ortadan kaldıran sebepler, teşebbüs, iştirak, içtima, zamanaşımı gibi ceza hukukunun bir çok temel ilkesine yer verilmiştir.

Yetkili Sulh Ceza Hakimi:

❑ Kabahatler Kanununun 22.md.4.fıkrasına göre 5271 Sayılı Ceza Muhakemesi Kanununun (CMK) yer bakımından yetki kuralları kabahatler açısından da geçerlidir. Yetki kuralını belirleyen CMK-12.md.1.fıkraya göre; ***ANA KURAL: suçun (kabahatin) işlendiği yer mahkemesi, davaya bakmaya genel yetkili mahkeme olacaktır.*** Ayrıca CMK-12.madde kapsamında; teşebbüs, kesintisiz suç ve zincirleme suçlar bakımından CMK-12/2.fıkra, suçun basılı bir eserle işlenmesi halinde CMK-12/3.fıkra, hakaret suçları, tutukluluk ve hükümlülük söz konusuysa CMK-12/4.fıkra; görsel ve işitsel yayınlarla işlenmesi durumunda 12/5.fıkra uygulama alanı bulacaktır.

❑ Diğer yandan özel yetki kurallarını düzenleyen CMK-13.md'ye göre; suçun işlendiği yer belli değilse, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi yetkili olacak; şüpheli veya sanığın Türkiye'de yerleşim yeri yoksa Türkiye'de en son adresinin bulunduğu yer mahkemesi yetkili olacak; Mahkemenin bu suretle de belirlenmesi olanağı yoksa, ilk usul işleminin yapıldığı yer mahkemesi yetkili olacaktır. Bunun yanında diğer özel hallerde yetkili mahkeme CMK-14, 15 ve 16. maddedeki kurallara göre bulunacaktır.

❑ Eğer Kurul kararlarına karşı, Kabahatler Kanunu kapsamında "Başvuru Yolu" öngörülmemiş ve CMK'nın yer bakımından yetki kurallarına atıf yapılmamış olsa idi; 2577 sayılı İdari Yargılama Usulü Kanunu ("İYUK") madde 32/1 uyarınca dava konusu olan idari işlemi veya idari sözleşmeyi yapan idari merciin bulunduğu yerdeki idare mahkemesi olarak, Kurul kararları Ankara İdare Mahkemelerinin önüne gelecek, maddi anlamda idare hukukunun, usul bakımından idari yargılama usul hukuku kurallarının uygulanması gerekecekti.

❑ Le point plus important à souligner ici; c'est le fait que le système introduit par la loi sur les délits n° 5326 est lié étroitement aux principes et règles généraux de procédure du droit pénal et du droit de procédure pénale, au-delà d'un acte administratif, tandis qu'il faudrait gérer un jugement selon les règles et procédures du droit de la juridiction administrative en terme des éléments de l'acte administratif et dans l'aspect procédural si le jugement etait effectué devant l'orde juridictions administratives conformément à la théorie de l'acte administratif surtout pour les affairs d'annulation de l'amende administrative. En fait, dans la loi sur les délits il s'agit de nombreux principes de base du droit pénal tels que; légalité, application en termes de temps et de lieu, le principe de responsabilité pénale, motifs légitimes, raisons qui éliminent la culpabilité, crime tentative, participation criminelle, le cumul des crimes et des peines et le délai de prescription.

le Juge pénale de paix compétent de lieu

❑ Les règles de compétence de lieu Code de procédure pénale (CPP) sont également valables en matière de délits conformément à l'article 22-IV de la loi sur les délits. Selon l'article 12-I du CPP déterminant la règle de compétence de lieu; ***RÈGLE PRINCIPALE: Le tribunal competent du lieu où le crime (délit) a été commis sera le tribunal competent général de lieu pour faire la poursuite***. En outre, dans le cadre de l'article 12 du CPP les dispositons suivantes seront appliquées: en matière de crimes tentés, de crimes continus et de crimes successifs, si le crime est commis avec une œuvre imprimée, s'il s'agit des crimes d'insultes ou des personnes détenues et prisonnières, et commises par des diffusions audiovisuelles.

D'autre part, selon l'article 13 du CPP, si le lieu du crime est inconnu, le tribunal de lieu où le suspect ou l'accusé a été arrêté sera competent, sinon le tribunal du lieu de résidence des suspects ou des accusés; si des suspects ou des accusés n'ont aucune résidence en Turquie, le tribunal de leurs adresses de domicile le plus récent en Turquie sera compétent de lieu; s'il n'a aucun moyen d'autre pour déterminer le tribunal competent, le tribunal du lieu où la première action procédurale a été introduite sera competent.

S'il n'était pas prévu « ***la Voie d'application***» dans le contexte de la loi sur les délits contre les décisions du comité de protection des données personnelles (CPDP) et s'il n'y avait pas de référence aux règles de compétence de lieu du CPP, selon la loi de procédure de juridiction administrative (LPJA) (Art.32/1); en tant que le tribunal administratif du lieu où se trouve l'autorité administrative qui fait l'acte ou le contrat administratif faisant l'objet du litige, les décisions de la CPDP seraient portées devant les tribunaux administratifs d'Ankara et ils devraient etre appliqué les règles du droit administratif en termes matériels et celles du droit procédurales de la juridiction administrative en termes de procédure.

Başvuru süresi

❑ İdari para cezalarına karşı başvuru yolunu kullanma (dava açma) süresi; 2577 sayılı İdari Yargılama Usulü Kanunundan (IYUK) farklı olarak, Kabahatler Kanununun 27.madde 1.fıkrasında yer alan hükme göre, kararın ***tebliğ veya tefhiminden itibaren en geç 15 gün olarak*** düzenlenmiştir. Bilindiği gibi, IYUK-7.maddesine göre dava açma süresi, özel kanunlarında ayrı süre gösterilmeyen hallerde Danıştay'da ve idare mahkemelerinde altmış ve vergi mahkemelerinde otuz gündür.

YAPILACAK BAŞVURU HARCA TABİ DEĞİLDİR.
(Kabahatler Kanunu Md.31)

Başvurunun İncelenmesi ve Karar:

❑ Başvuru üzerine Sulh Ceza hâkimliği öncelikle Kabahatler Kanunun 28.madde 1.fıkrası gereğince; başvuru süresinin geçirilip geçirilmediği, başvuruya bakmaya yetkili olup olmadığı, başvuru sahibinin başvuru yapmaya hakkı olup olmadığı konularında ön inceleme yapar, ön inceleme sonunda bu şartlar karşılanmıyorsa duruma göre, ya başvurunun yetkili sulh ceza hakimine gönderilmesine veya başvurunun usulden reddine kararı verir. Başvuru içeriğinde bu şartlar karşılanıyorsa başvurunun usulden kabulüne karar verir.

❑ Usulden kabul edilen bir başvuru dilekçesinin bir örneği 28.madde 2.fıkrası gereğince; Kişisel Verileri Koruma Kuruluna tebliğ edilir, Kurul bu dilekçeye karşı cevaplarını, idari para cezasına ilişkin dosyayla birlikte tebliğ tarihinden itibaren 15 gün içinde Sulh Ceza Hâkimine gönderir.

❑ Sulh Ceza Hâkimi, başvuru sahibine Kurul'un cevap dilekçesini tebliğ eder; talep üzerine veya re'sen tarafları çağırarak belli bir gün ve saatte dinleyebilir. Hâkim, ilgilileri dinledikten ve bütün delilleri ortaya koyduktan sonra aleyhinde idari yaptırım kararı verilen ve hazır bulunan taraflara son sözünü sorar ve son kararını hazır bulunan tarafların huzurunda açıklar.

❑ Sulh Ceza Hakimi, **"başvurunun reddine"**, **"idarî yaptırım kararının kaldırılmasına"** veya idarî para cezasının miktarını azaltarak **"başvurunun (kısmen) kabulüne"** karar verebilir. (Kabahatler Kanunu 28.maddesi 9.fıkra)

❑ Üçbin Türk Lirası dâhil (*(2020 yılı yeniden değerleme oranına göre 5.404 TL)* idarî para cezalarına karşı başvuru üzerine verilen kararlar kesindir. (Kabahatler Kanunu 28.maddesi 10.fıkra)

Le délai d'application

❑ le Délai du recours (poursuite) contre les amendes administratives est considéré comme un délai de 15 jours au plus tard à compter de la notification ou prononciation de la décision selon la disposition de l'article 27-I de la loi sur les délits différemment à la loi de procédure de juridiction administrative (LPJA) n° 2577. Le délai du recours selon l'article 27 de la LPJA c'est 60 jours pour les tribunaux administratifs et le Conseil d' État (comme un tribunal de première instance) et c'est 30 jours pour les tribunaux fiscaux, dans les cas où aucun délai distinct n'est spécifié dans leurs lois particulières

PAS DE FRAİS DE JUSTİCE POUR LES APPLİCATİONS
(Art.31 de la loi sur les délits)

Examination de l'application et la décision

❑ Le juge pénal de paix, premièrement, conformément à l'article 28-I, de la loi sur les délits; procède à un examen préliminaire pour savoir si le délai de l'application est expiré, si le juge soi-même a compétence à examiner l'application, si le demandeur a le droit de présenter une telle demande; et si ces conditions ne sont pas remplies à l'issue de l'examen préliminaire, il décide de renvoyer au juge pénal de paix compétent de lieu ou de rejeter l'application pour déroulement formel de la procédure. Si elles sont remplies dans le contenu de l'application, il décide à recevabilité formelle de l'application.

❑ Un exemplaire de la requête reçue formellement est notifié au comité de protection des données personnelles (CPDP) selon l'article 28-II de la loi sur les délits, le CPDP adresse ses réponses à cette requête au juge pénal de paix dans les 15 jours à compter de la date de notification, avec le dossier sur l'amende administrative en question.

❑ Le juge pénal de paix notifie la réponse du CPDP au demandeur de la requête; Il peut écouter les parties à un certain jour et une certaine heure precise en les appelant à l'audience sur demande ou de son propre gré. Le juge, après avoir écouté les parties et présenté toutes les preuves, Il demande son dernier mot aux parties contre lesquelles une décision de sanction administrative a été prise et qui sont présentes, et finalement prononce sa décision en présence des parties présentes.

❑ Le juge pénal de paix peut décider **"le rejet de la demande"**, **"l'annulation de la décision de sanction administrative"** ou **"l'acceptation (partielle) de la demande"** en réduisant le montant de l'amende administrative. (Loi sur les délits, Art 28/9)

❑ Les décisions concernant les amendes administratives y compris trois mille livres turques sont définitives. (5,404 ₺ selon le taux de réévaluation pour 2020), (Loi sur les délits, Art 28/10)

Başvuru Konusu Olabilecek Hatalı İdari Uygulamalar:

- İdari Para Cezası düzenlenirken savunma hakkının kullandırılmaması,
- İdari Para Cezası Kararında gerekçe olmaması,
- İdari Para Cezası Kararının tarafsızlık ilkesine aykırı olarak alınması,
- İdari Para Cezası Kararını veren idari organın, yaptırım içeren hükümdeki alt ve üst sınır arasındaki takdir yetkisini hatalı kullanması,
- İdari Para Cezası Kararının yetkili idari organ dışında (Kabahatler Kanununun İdarî yaptırım kararı verme yetkisini düzenleyen 22.maddenin 2.fıkrasına göre ***"Kanunda açık hüküm bulunmayan hallerde ilgili kamu kurum ve kuruluşunun en üst amiri bu konuda yetkilidir."*** 6698 sayılı Kişisel Verilerin Korunması Kanununda bu konuda açık bir düzenleme bulunmadığından, bu durumda idari para cezası kararlarının ***Kurul Başkanı*** tarafından verilmesi gerekmektedir.) başka bir kişi veya organ tarafından verilmesi,
- Kabahatler Kanunu 20.maddede yer alan soruşturma zaman aşımı sürelerinin aşılması,
- Kabahatler Kanunu 21.maddedeki yerine getirme zamanaşımı sürelerinin aşılması,
- İşlenen fiilin, 6698 sayılı Kişisel Verilerin Korunması Kanununda yazan kabahatlerin tanımına uymaması (tipiklik şartını taşımaması),
- ***Kişisel Verilerin Korunması Kurulunun*** İdari Para Cezalarında kıyas yasağına aykırı (kanunilik ilkesine aykırılık) olarak idari para cezası kararı vermesi,
- Aynı fiilden dolayı çifte cezalandırma yasağına aykırı idari para cezası kararı vermesi,
- Esasa ve Usule İlişkin Diğer Hatalı Uygulamalar.

Sulh Ceza Hâkimi Kararına Karşı İtiraz Kanun Yolu

- Hakkında idari para cezası uygulanan veri sorumlusunun 15 günlük bu süreyi, sulh ceza hâkimine başvurmadan geçirmesi durumunda idari para cezası kararı kesinleşir. Eğer veri sorumlusu süresi içinde Sulh ceza hâkimine başvurmuş, ancak başvurusu kabul görmemişse, Kabahatler Kanunu 29.maddesi 1.fıkrasındaki "Mahkemenin (Sulh Ceza Hakimi) verdiği son karara karşı, CMK'ya göre itiraz edilebilir. Bu itiraz, kararın tebliği tarihten itibaren en geç yedi gün içinde yapılır." şeklindeki hükmün yaptığı atfa istinaden CMK hükümlerine göre itiraz yoluna başvurabilir. İtiraz üzerine

Mal administration à faire l'objet d'une application:

- L'absence de l'exercice du droit de défense lors de l'émission d'une amende administrative,
- Manque des motifs de la décision d'amende administrative,
- Prise de la décision d'amende administrative en violation du principe d'impartialité,
- Mauvaise usage du pouvoir discrétionnaire entre la limite inférieure et supérieure de la disposition relative à la sanction par l'organe administratif qui décide de l'amende administrative,
- Prise de la décision d'amende administrative par une autre personne ou un organisme autre que l'organisme administratif autorisé. (Selon l'article 22-II de la loi sur les délits ***«dans les cas où il n'y a pas de disposition explicite dans la loi, le supérieur hiérarchique de l'institution et de l'organisation publique concernée est autorisé à cet égard.»*** Comme il n'y a aucune réglementation explicite à ce sujet dans la loi sur la protection des données personnelles n° 6698, dans ce cas les décisions relatives aux amendes administratives devraient être prises par le ***président du conseil***.)
- Dépassement du délai de prescription d'enquête prévu à l'article 20 de la loi sur les délits.
- Dépassement du délai de prescription d'exécution prévu à l'article 21 de la loi sur les délits.
- Inconformité (de typicité) de l'acte commis à la définition des délits dans la loi sur la protection des données personnelles.
- Prise de la décision d'amende administrative contre l'interdiction de l'analogie (contre le principe de légalité) par le comité de protection des données personnelles.
- Prise de la décision d'amende administrative contre l'interdiction de la double punition pour le même acte.
- D'autres mal pratiques substantiels et procéduraux.

La voie de recours «Objection» contre le verdict du juge pénal de paix

Lorsque le responsable du traitement qui fait l'objet d'amendes administratives dépasse ce délai de 15 jours sans s'adresser au juge pénal de paix, la décision d'amendes administratives devient définitive. Si le responsable du traitement a saisi au juge pénal de paix dans le délai imparti, mais que sa demande n'a pas été acceptée, une objection peut être formulée conformément aux dispositions du CPP, sur la base de la référence de l'article 29-I de la loi sur les délits ***«une***

verilen kararlar CMK-Md.271, f.4 gereğince kesin olduğu için bu kararlar aleyhine istinaf ve temyiz kanun yolu kullanılamaz.

❑ Sulh Ceza Hâkimliklerinin kararlarına itiraz halinde itirazı incelemeye yetkili merciler CMK-268.md.3 fıkra, a) bendinde düzenlenmiştir:

> ***"Sulh ceza hâkimliği kararlarına yapılan itirazların incelenmesi, o yerde birden fazla sulh ceza hâkimliğinin bulunması hâlinde, numara olarak kendisini izleyen hâkimliğe; son numaralı hâkimlik için bir numaralı hâkimliğe; ağır ceza mahkemesinin bulunmadığı yerlerde tek sulh ceza hâkimliği varsa, yargı çevresinde görev yaptığı ağır ceza mahkemesinin bulunduğu yerdeki sulh ceza hâkimliğine; ağır ceza mahkemesinin bulunduğu yerlerde tek sulh ceza hâkimliği varsa, en yakın ağır ceza mahkemesinin bulunduğu yerdeki sulh ceza hâkimliğine aittir."***

<u>İdari Para Cezalarının Verilmesinde Zamanaşımı Süreleri</u>

❑ 6698 sayılı Kişisel Verilerin Korunması Kanununda (KVKK) idari para cezalarının verilmesine ve infazına dair bir hüküm bulunmamakla birlikte, genel kanun olması niteliği sebebiyle 5326 sayılı Kabahatler Kanunu uygulama alanı bulmaktadır. Kabahatler Kanunu zaman aşımını; 20.maddede **soruşturma zamanaşımı** ve 21.maddede **yerine getirme zamanaşımı** olarak iki şekilde düzenlemiştir.

❑ Kabahatler Kanunu 20.maddeye göre, "**Soruşturma zamanaşımı süresi**; a)Yüzbin Türk Lirası veya daha fazla idarî para cezasını gerektiren kabahatlerde **beş,** b) Ellibin Türk Lirası veya daha fazla idarî para cezasını gerektiren kabahatlerde **dört,** c)Ellibin Türk Lirasından az idarî para cezasını gerektiren kabahatlerde **üç yıldır**." Soruşturma zamanaşımı süresi, idari para cezasının kanunda gösterilen üst sınırı esas alınarak belirlenir. Kabahat fiilinin işlenmesinden itibaren maddede belirtilen süreler içerisinde Kişisel Verileri Koruma Kurulu tarafından söz konusu kabahatler hakkında gereken idari yaptırımın uygulanmaması halinde bu sürelerden sonra soruşturma, zamanaşımına uğrayacak ve artık herhangi bir idari yaptırım uygulanamayacaktır. Soruşturma zamanaşımı kabahat fiilinin işlenmesi ya da neticenin gerçekleşmesinden itibaren işlemeye başlayacaktır.(Kabahatler Kanunu 20.madde 4.fıkra)

❑ Kesinleşen bir idari para cezalarının Kabahatler Kanunu 21.madde 2.fıkrada düzenlenen yerine getirme zamanaşımı süreleri içinde yerine getirilmesi gerekmektedir: "Yerine getirme zamanaşımı süresi; a)Ellibin Türk Lirası veya daha fazla idarî para cezasına karar verilmesi halinde **yedi,** b)Yirmibin Türk Lirası veya

objection peut être formulée conformément au CPP contre le verdict du juge. Cette objection est formulée dans un délai de 7 jours au plus tard à compter de la notification du verdict». Étant donné que les décisions prises suite à l'objection sont définitives conformément à l'article 271-IV du CPP, les voies de recours d'appel et de cassation sont fermés contre ces décisions.

❑ En cas d'objection aux verdicts des juges pénales de paix, les juges compétents pour examiner l'objection sont réglementés par l'alinéa III.a de l'article 268 du CPP:

> ***«La décision d'un juge pénal de paix peut être contestée, là où il existe plusieurs juridictions de ce type, devant le juge pénal de paix portant le numéro suivant; et devant le juge pénal de paix au numéro (I) pour celui du dernier numéro; là où il n'existe qu'un seul juge pénal de paix dans le lieu où aucune cour d'assises n'existe, devant le juge pénal de paix se trouvant dans la zone de compétence de la cour d'assises la plus proche; là où il n'existe qu'un seul juge pénal de paix dans la zone de compétence de la cour d'assises, devant le juge pénal de paix se trouvant dans le lieu plus proche où il se trouve une cour d'assises. »***

<u>Le délai de prescription pour l'émission des amendes</u>

❑ Bien qu'il n'y ait aucune disposition concernant l'imposition et l'exécution d'amendes administratives dans la loi sur la protection des données personnelles (LPDP), la loi sur les délits n° 5326 est applicable en tant qu'une loi générale. Dans la loi sur les délits le délai de prescription est réglementé en deux manières: le délai de **prescription d'enquête** selon l'article 20 et le délai de **prescription d'exécution** selon l'article 21.

❑ Selon l'article 20 de la loi sur les délits, «***les délais de prescription d'enquête*** sont: a) ***Cinq ans*** pour les délits nécessitant une amende administrative de 100.000 ₺ ou plus, b) ***Quatre ans*** pour les délits nécessitant une amende administrative de 50.000 ₺ ou plus, c) ***Trois ans*** pour les délits nécessitant une amende administrative de moins de 50.000 ₺». Le délai de prescription d'enquête est déterminée en fonction du maximum des amendes administratives indiqué dans la loi. Dans le cas ou le Comité de protection des données personnelles n'applique pas des sanctions administratives nécessaires concernant les délits en question à partir de la commission de l'acte de délit dans les délais spécifiés dans l'article, après ces délais, l'enquête sera prescrite et aucune sanction administrative ne sera imposée. Le délai de prescription d'enquête débutera après que l'acte délictueux aura été commis ou que le résultat sera atteint (Art.20/4 de la loi sur les délits).

❑ Les amendes administratives définitives doivent être exécutées dans les délais de prescription prévus à l'article 21-II de la loi sur les délits: «les délais de prescription

daha fazla idarî para cezasına karar verilmesi halinde **beş,** c)Onbin Türk Lirası veya daha fazla idarî para cezasına karar verilmesi halinde **dört**, d)Onbin Türk Lirasından az idarî para cezasına karar verilmesi halinde **üç yıldır**."

❑ Kişisel Verileri Koruma Kurulu tarafından verilen İdari para cezalarının kesinleşmesi üç şekilde gerçekleşebilir: a) Hakkında idari para cezası uygulanan gerçek veya tüzel kişinin, Kabahatler Kanunu 27.md. gereğince, kararların tefhim veya tebliğinden itibaren on beş gün içerisinde sulh ceza hâkimine başvurmaması halinde kesinleşmesi, b) Sulh ceza hâkimine süresi içinde başvurulduğu halde, Sulh ceza hâkiminin "başvurunun reddine" veya "idari para cezası miktarını azaltarak başvurunun kısmen kabulüne" karar vermesi halinde, Kabahatler Kanunu 29.md. gereğince kararın kendisine tebliğinden itibaren yedi gün içerisinde CMK hükümlerine göre İtiraz yoluna başvurmaması halinde kesinleşmesi c) Süresi içinde İtiraz yoluna başvurduğu halde, itiraza bakan sulh ceza hâkimi tarafından itirazın reddedilmesi kararı verilmesi halinde kesinleşmesi.

❑ Kabahatler Kanunu 21.madde 4.fıkraya göre ise "Zamanaşımı süresi, kararın kesinleşmesinin rastladığı takvim yılını takip eden takvim yılı başından itibaren işlemeye başlar."

d'exécution sont; a) **sept ans** en cas d'amende administrative de 50.000 ₺ ou plus, b) **cinq ans** en cas d'amende administrative de 20.000 ₺ ou plus, c) **quatre ans** en cas d'amende administrative de 10.000 ₺ ou plus, d) **trois ans** en cas d'amende administrative de moins de 10.000 ₺».

❑ Les amendes administratives infligées par le comité de protection des données personnelles peuvent être définitives de trois manières: a) dans le cas ou la personne physique ou morale condamnée à des amendes administratives ne s'applique pas au juge pénal de paix dans les quinze jours suivant la notification ou la prononciation des décisions de sanction selon l'article 27 de la loi sur les délits, elles deviennent définitives; b) bien qu'il soit une application au juge pénal de paix en temps voulu et au cas où le juge pénal de paix déciderait de "rejeter la demande" ou "d'accepter partiellement la demande en réduisant le montant de l'amende administrative" et s'il s'agit d'un manque de l'objection formulée selon les dispositions du CPP avec référence de l'article 29 de la loi sur les délits dans les sept jours à compter de la notification de la décision, les décisions de sanction deviennent définitives; c) lorsque la décision de rejet de l'objection soit rendue par le juge pénal de paix même s'il s'agit d'une application de l'objection en temps voulu, les décisions de sanction deviennent définitives.

❑ Selon l'article 21-IV de la loi sur les délits "Le délai de prescription commence au début de l'année civile suivant l'année civile au cours de laquelle la décision devient définitive."

Kişisel Verilerin İşlenmesine Egemen Olan İlkeler ve Bu Kapsamda Verilen KVK Kurul Kararları

Stj.Av. Tolga Koncagül

Giriş

Kişisel Verinin Tanımı ve Kişisel Verilerin Korunmasını Talep Hakkının Dayanağı

❑ Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişilere ait her türlü bilgi olarak tanımlanır. Gerçek kişiler için kişiler verilerin korunmasını talep etme hakkı dayanağını Anayasa'nın 20. maddesinde ve Avrupa Birliği Temel Haklar Bildirgesinin 8. maddesinden alan bir temel haktır. Hukuk düzenimizde bu temel hakkı etkili bir şekilde koruyabilmek için Avrupa Birliği'nin 1995 tarih ve 46 sayılı Veri Korunması Yönergesi esas alınarak oluşturulan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), Parlamentoda 24.03.2016 tarihinde kabul edilmiş ve 07.04.2016 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

❑ Kişisel veriler şahıs varlığı hakkı olup kapsamı KVKK madde 2' de şu şekilde belirtilmiştir: ***''Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.''*** Maddeden de anlaşıldığı üzere kişisel verilerin korunmasını talep hakkı gerçek kişilere tanınmış bir hak olup tüzel kişiler ve vefat eden kişiler bu korunmanın kapsamında değildir. KVKK'da düzenlenen özel hükümler dışında Türk Medeni Kanununda da kişilik haklarını koruyan genel hükümler düzenlenmiş olup kişisel veriler bu hükümlere göre de korunabilir.

❑ Kişisel verileri koruyan tüm kanun hükümleri kişisel verileri koruma hukukunun genel ilkelerine göre yorumlanır. Doktrinde kişisel veriler ikili bir ayrıma tabi tutulmuştur. Buna göre kişisel veriler, özel nitelikli kişisel veriler ve genel nitelikli kişisel veriler olarak ikiye ayrılır. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli verilerdir. KVKK 6.maddede özel nitelikli kişisel verilerin neler olduğu sayılmıştır. 6.maddede belirtilen hususlar sınırlı sayı ilkesine tabidir. Bu kapsama giren her türlü veri özel nitelikli kişisel veri kapsamında değerlendirilir. Genel nitelikli kişisel veriler ise özel nitelikli kişisel veri kapsamına girmeyen her türlü veri olarak değerlendirilir. Teknolojik yeniliklerle ortaya çıkan ve özel nitelikli kişisel veri kapsamını düzenleyen maddeye eklenmeyen her türlü veri genel nitelikli kişisel veri kapsamına girer. Özel nitelikli kişisel verilerden farklı olarak genel nitelikli kişisel verilerde sınırlı sayı ilkesi geçerli değildir.

Principles Governing the Processing of Personal Data and Board Decisions Made Within This Scope

Abstract

Definition of personal data and the basis of the right to request protection of personal data

❑ Personal data is defined as all kinds of information belonging to an identified or identifiable natural person.Personal processing, on the other hand, defined as obtaining, recording, storing, preserving, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use, in whole or in part or as part of any data recording system.For natural persons, it is a fundamental right that derives its basis from Article 20 of the Constitution and Article 8 of the European Union Declaration of Fundamental Rights. Law No. 6698 on the Protection of Personal Data (LPPD), which was established on the basis of the Protection Directive, was accepted by the Parliament on 24.03.2016 and entered into force after being published in the official newspaper on 07.04.2016.

❑ Personal data is the right to be a person and its scope is stated in Article 2 of the LPPD as follows: ***''The provisions of this Law are natural persons whose personal data are processed and the natural and legal persons who processes this data completely or partially automatically or by non-automatic means provided that they are part of any data recording system.''*** As it can be understood from the article, the right to request the protection of personal data is a right granted to natural persons, legal entities and deceased persons are not covered by this. Apart from the special verdicts regulated in the LPPD, general verdicts protecting personal rights are also regulated in the Turkish Civil Law and personal data can also be protected according to these law articles.

❑ All the articles of the law protecting personal data are interpreted according to the general principles of the law on protection of personal data. In the doctrine, personal data are divided into two categories: Personal data is divided into "special categories of personal data" and "general personal data". Listed in Arcticle 6, "Special categories of personal data" entails personal data relating to the ethnic origin, political opinion, philosophical belief, religion, sect or oher belief, clothing, membership to associations, foundations or trade union, health, sexual life, convictions and security measures and the biometric and genetic data are deemed to be special ctegories of personal data. The matters stated in the article are subject to the limited number principle. All kinds of data covered by this are considered within the scope of "special categories of personal data" . General personal data, on the other hand, is considered as any data that does not fall within the scope of "special categories of personal data" . All kinds of data that emerge with technological innovations and are not added to the article regulating the

Kişisel verilerin işlenmesi tanımı ve şartları

❑ Kişisel verilerin işlenmesi tanımı KVKK 3. maddesinin e bendinde belirtilmiş olup maddede: ***"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"*** olarak tanımlanmıştır.

❑ Kişisel verilerin işlenme şartları da aynı kanunun 5. maddesinde belirtilmiştir ve sınırlı sayı ilkesine tabidir. Buna göre kişisel verilerin işlenebilmesi için ilgili kişinin açık rızası, kanunlarda açıkça öngörülmesi, bir sözleşmenin kurulması veya ifasıyla doğrudan ilgiliyse sözleşmenin taraflarına ait kişisel verilerin saklanması gerektiği hallerde, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması halinde, ilgili kişinin kendisi tarafından kamuoyuna açıklandığı durumlarda, bir hakkın belirlenmesi, kullanılması veya korunması için veri işlemenin zorunlu olduğu hallerde, ilgili kişinin temel hak ve özgürlüklerini zedelemediği sürece veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olduğu haller kişisel veri işleme şartlarını oluşturur.

Kişisel Verilerin İşlenmesinde Rıza

❑ KVKK'ya göre rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. 95/46 EC sayılı Avrupa Birliği Direktifinde açık rıza; ***"ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı"*** şeklinde anlaşılmakta olup, Avrupa Birliği'nde yalnızca özel nitelikli verilerin işlenmesi için açık rıza şartı aranmıştır. Ülkemizde kural olarak her türlü kişisel verinin işlenmesi için açık rızaya ihtiyaç duyulmaktadır. Bu açıdan Kanununumuz, Avrupa Birliği düzenlemelerine kıyasla daha koruyucu niteliktedir. Rıza açıklaması veri işleyene gerçekleştireceği fiil konusunda yol gösterici niteliktedir. Kişi rıza açıklaması ile aslında veri işleyene kendi hukuksal değerine ilişkin verdiği kararı bildirir.

❑ Rıza açıklaması ilgilinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme şeklini belirtir ve süresini de belirlemesini sağlar. Ayrıca açık rıza kural olarak yazılı şekle tabi değildir. Elektronik

scope of "special categories of personal data" within the scope of general personal data. Unlike "special categories of personal data" , the limited number principle does not apply to general personal data.

Definition and conditions of processing personal data

❑ The definition of the processing of personal data is specified in the clause e of Article 3 of the LPPD, in the article: ***Obtaining, recording, storing, preserving, changing, reorganizing, explaining personal data completely or partially automatically or non-automated provided that it is part of a data recording system. Any transaction performed on data such as transferring, taking over, making available, classifying or preventing their use.***

❑ The conditions for the processing of personal data are also specified in Article 5 of the same law and are subject to the principle of limited number. In cases where it is necessary for the protection of the life or body integrity of the person or someone else who is unable to disclose his consent due to his consent or whose consent is not legally valid, if it is necessary for the data controller to fulfill his legal obligation, in cases where it is disclosed to the public by the person concerned, the determination and use of a right data processing is mandatory for the legitimate interests of the data controller, as long as it does not damage the fundamental rights and freedoms of the person concerned.

Definition of Consent and Giving Consent to the Processing of Personal Data

❑ According to LPPD, consent means giving consent to the processing of the data that the person has, at their own request or upon the request from the other party.In European Union Directive 95/46 EC explicit ***consent is understood as a declaration of consent given by the data subject freely, having sufficient information on the subject, open to no hesitation and limited only to that process*** . European Union, explicit consent for processing is only required on data includes special nature. In our country, explicit consent is required for the processing of all kinds of personal data. In this respect, our Law is more protective compared to the European Union regulations. The consent disclosure is a guide for the data processor about the action to be taken. The person actually notifies the data processor the decision he has made regarding his own legal value with the consent statement.

❑ The consent disclosure allows the person concerned to determine the limits, scope, realization method and duration of the data permitted to be processed. Other than the exceptions provided for by law, explicit consent is not subject to written form. Explicit consent can also be obtained electronically. If the personal data is processed on the basis of one of the conditions other than the

ortamda da açık rıza alınabilir. Kişisel veri ilgilinin açık rızası haricindeki şartlardan birine dayanarak işleniyorsa ilgili kişinin rızası aranmaz. Dikkat edilmesi gereken husus açık rıza dışı bir şarta dayanarak veri işlenebiliyorken veri işlemenin açık rızaya dayandırılarak işlenmesi hakkın kötüye kullanımı sayılacaktır. Örnekle açıklayacak olursam işverenin çalışanı teşvik etmek amacıyla bir yıllığına ikramiye verecek olması ve bunun takibi için ikramiye alanların kaydının tutulması için işçilerinden izin alması. Örnekte işveren veri sorumlusunun meşru menfaati şartından faydalanabilecekken açık rıza şartına dayanmış olursa işçinin rızayı geri çekmesi halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem teşkil edecektir. Bu sebeple açık rıza şartı haricindeki şartlardan biri sağlanıyorsa açık rıza şartına başvurulmamalıdır. Son olarak kişisel veri faaliyetinin amacı birden fazla kişisel veri işleme şartına dayanabilir.

İlkeler

Genel olarak

❑ Kişisel verilerin toplanması ve işlenmesine ilişkin ilkeler AB yönergesinden iktibas edilmiş olup KVKK madde 4'te düzenlenmiştir. Buna göre:

> ***"Genel ilkeler***
> ***MADDE 4- (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.***
> ***(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:***
> ***a) Hukuka ve dürüstlük kurallarına uygun olma.***
> ***b) Doğru ve gerektiğinde güncel olma.***
> ***c) Belirli, açık ve meşru amaçlar için işlenme.***
> ***ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.***
> ***d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."***

olarak maddede uyulması zorunlu beş ilkeden bahsedilmiştir.

❑ Verilerin korunması için elzem olan bu ilkeler birbirleri ile bağlantılıdır ve bu ilkelere uyulması zorunludur. Bu durum kişisel verilerin korunması kapsamında bütün yasal düzenlemelere uygunluk açısından da temel teşkil etmektedir. Yukarıda anlatılan ilkeler arasındaki bağlantıyı daha rahat anlaşılabilmesi için örneklendirerek şu şekilde açıklayabiliriz; Hukuka ve dürüstlük kuralına uygun olma ilkesi sadece kişisel verilerin korunmasına özgü bir ilke olmayıp hukukun her alanında elzem bir ilkedir. Hukuka ve dürüstlük kuralına uygun olmayan bir veri işleme faaliyetinin doğru ve gerektiğinde güncel olma ilkesine uygun olması bir anlam

express consent of the person concerned, the consent of the person concerned is not sought. The point to be considered is that data processing can be processed on the basis of an explicit non-consent condition, but the processing of data based on explicit consent will be deemed to be an abuse of the right. For example, the employer will give a bonus for one year to encourage the employee and for this, the employer asks permission to keep the record of the personal information of the one who gets the bonus. In that case employer is able to benefit from the legitimate interest of the data controller but employer based on the condition of express consent, that means ıf the employee withdraws the consent, the data controller's continuing the data processing activity based on one of the other personal data processing conditions will constitute a transaction against the law and the rules of honesty. Finally, the purpose of personal data activity may be based on more than one personal data processing condition.

Principles

General Scope

❑ The principles regarding the collection and processing of personal data are derived from the EU directive and regulated in Article 4 of the LPPD. Article 4 says;

> ***"General principles***
> ***Article 4-(1) Personal data can only be processed in accordance with the procedures and principles stipulated in this Law and other laws.***
> ***(2) It is mandatory to comply with the following principles in the processing of personal data:***
> ***a) Compliance with the law and good faith.***
> ***b) Being accurate and up-to-date when necessary.***
> ***c) Processing for specific, explicit and legitimate purposes.***
> ***d) Being connected, limited and measured for the purpose for which they are processed.***
> ***e) Being kept for the period stipulated in the relevant legislation or required for the purpose for which they are processed"***

❑ These principles, which are essential for the protection of data, are interlinked and these principles must be followed. This situation also constitutes the basis in terms of compliance with all legal regulations within the scope of the protection of personal data. In order to understand the connection between the principles described above more easily, we can explain as follows; The principle of compliance with the law and the rule of honesty is not only a principle specific to the protection of personal data, it is an essential principle in all areas of law. The general principles listed in the article on the protection of personal data do not contain concrete, rigid rules. These

ifade etmeyecektir. Kişisel verilerin korunmasına ilişkin maddede sayılan genel ilkeler somut, katı kurallar içermemektedir. Bu ilkeler veri koruma düzenlemelerine uygunluğa ilişkin kuralları içermektedir. Bu ilkelere uyulmaması hukuka aykırılık teşkil eder.

Bu ilkeler sırayla aşağıda açıklanmıştır.

Hukuka ve dürüstlük kuralına uygun olma ilkesi:

❑ Hukuk sistemimizdeki diğer alanlarda olduğu gibi burada da dikkate alınmaktadır. Bu ilke kısaca hukuk devleti olmanın bir gereği olup, Medeni kanun 2.maddede belirtilen dürüstlük kuralına uygun şekilde hareket edilmesi ayrıca veri işleyen kişilerin kötü niyetli hareket etmemesi gerekir. Verinin işlenmesi "açık rıza" veya bunun dışında kanunlarda işlemenin açık bir şekilde izin verildiği hukuka uygunluk sebeplerinden birisi kapsamında işlenmesi halinde veri işleme hukuka uygun hale gelir. Veri sorumlusu, veri işlemedeki amacına yönelik işlem yaparken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almalıdır. İlgili kişinin beklemediği ve beklemesinin de gerekmediği sonuçların ortaya çıkmasını önleyici eylem ve işlemlerden kaçınması gerekir. İlkenin bir gereği olarak ayrıca ilgili kişi için söz konusu veri işleme faaliyetinin şeffaf olması ve veri sorumlusunun bilgilendirme ve uyarı yükümlülüklerine uygun hareket etmesi de gerekmektedir. Veri işleyenin ayrıca hukuka aykırı veri işlenmesini önlemek için gerekli tedbirleri de alması gerekmektedir.

❑ Bu konuya ilişkin Kişisel Verileri Koruma Kurulunun ***İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi*** *konulu 07/11/2019 Tarihli ve 2019/331 Sayılı Kararında "Şikâyetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Şirket tarafından Şikâyetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı, diğer bir deyişle Şikâyetçinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine Şirket faaliyetlerine ilişkin randevu talebi ile Şikâyetçinin arandığı anlaşıldığından, Şirket tarafından gerçekleştirilen veri işleme faaliyetinin 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (d) bendi çerçevesinde değerlendirilemeyeceği kanaatine varılmış olup, bu kapsamda* ***Şirketin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almayarak*** *Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı davranmış olması nedeniyle Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına karar verilmiştir."* denmiştir.

principles include rules on compliance with data protection regulations. Failure to comply with these principles constitutes unlawfulness.

These principles are explained below in order.

Compliance with the law and good faith

❑ As in other areas in our legal system, it is taken into account here. If the data is processed within the scope of "explicit consent" or one of the reasons for compliance with the law for which the processing is explicitly permitted by the laws, the data processing becomes legal. The data controller should take into account the interests and reasonable expectations of the data subjects while performing the data processing purposes. The person concerned should avoid actions and procedures that prevent the occurrence of unexpected and unnecessary results. As a requirement of the principle, it is also necessary for the data subject to be transparent for the data subject and to act in accordance with the information and warning obligations of the data controller.

❑ One of the decisions of the Personal Data Protection Board regarding this issue is given 07/11/2019 and numbered 2019/331. *The subject of the violation is* ***the processing of personal data made public by the relevant person for purposes other than publicization****, the Complainant's personal data is accessed from the website that was previously made public by the Company. Since it is understood that the information is not used for the purpose of presenting and publicizing the information on the website, in other words, it is not attempted to reach the Complainant in order to benefit from the professional competence of the Complainant, on the contrary, it is understood that the Complainant is called with an appointment request regarding the Company's activities, It has been concluded that the data processing activity carried out by the Company cannot be evaluated within the framework of subparagraph (d) of paragraph (2) of Article 5 of the Law on the Protection of Personal Data No.6698, and within this scope, the* ***Company shall be required to provide any necessary security level in order to prevent the illegal processing of personal data****. It has been decided to impose an administrative fine of 100,000 TL on the Company in accordance with sub-clause (b) of paragraph (1) of Article 18 of the Law, due to the fact that it violated sub-paragraph (a) of paragraph (1) of Article 12 of the Law by not taking any technical and administrative measures.*

Doğru ve gerektiğinde güncel olma ilkesi

❑ Doğru ve gerektiğinde güncel olma ilkesi beraberinde aktif özen yükümlülüğünü getirir. Aktif özen yükümlülüğünün gereği olarak veri sorumlusunun ilgili kişinin verilerin düzeltilmesini talep etmesine imkan tanıyacak koşulları sağlaması gerekir. Kişisel verilerin doğru ve güncel olması gerektiğine atıfta bulunan bu ilke Kanunda öngörülen ilgili kişinin, verilerin düzeltilmesini talep etme hakkının bir sonucudur.

❑ Kişisel verilerin doğru ve güncel bir şekilde tutulması hem veri sorumlusunun çıkarlarıyla bağdaşmakta hem de ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da önem arz etmektedir. Örneğin kişinin yaşam yerine ilişkin bir verinin yanlış tutulması sonucunda hatalı sonuçlardan ötürü başvuru vb. işlemlerde adresin önem arz ettiği durumlarda sorun teşkil edebilir.

Belirli açık ve meşru amaçlar için işlenme ilkesi

❑ Belirli açık ve meşru amaçlar için işlenme ilkesi, ilgili kişisel veri işlemlerinin açık bir şekilde verisi işlenen taraf tarafından anlaşılabilmesi, kişisel veri işleme faaliyetlerinin hangi hukuki dayanağa sahip olduğunun belirli olması, kişisel veri işleme faaliyeti ve faaliyetin gerçekleştirilme amacının belirliliğinin açıkça ortaya konmasını sağlamak amacıyla kanunda düzenlenmiştir. Kanunda açıkça belirtilmese de hesap verilebilirlik ilkesiyle bu ilke iç içedir. Amacın açık ve meşru olması şarttır.

❑ Örneğin online bir mağazanın müşterinin adı soyadı haricinde TC kimlik no'su nu da veri olarak işlemesi bu meşru değildir bu sebeple bu ilkeye aykırıdır. Bu ilkeye başka bir örnek ise Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Kararıdır. Kararda; *Amazon Turkey Perakende Hizmetleri Limited Şirketince işlenen kişisel veriler hakkında yapılan başvuru sonucunda alışveriş yapabilmek için zorunlu olan üye hesabı oluşturulması amacıyla "Kullanım ve Satış Şartları"nı kabul ederek elektronik iletişim izni verilmiş sayılmanın özgür irade ile verilmiş bir açık rıza olarak değerlendirilemeyeceği, bu sebeple kişisel verilerin işlenmesinde "hukuka ve dürüstlük kurallarına uygun olma", "**belirli, açık ve meşru amaçlar için işlenme**" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uyulmadığından ve KVKK 8-9.cu maddelerinin ihlaliyle beraber veri sorumlusu tarafından Kanunun 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmemesinden dolayı Kanunun 18'inci maddesinin (1) numaralı maddesinin (b) bendi kapsamında 1.100.000 TL idari para cezası uygulanmasına, karar verilmiştir.''*

The principle of being accurate and up-to-date when necessary

❑ The principle of being accurate and up-to-date when necessary brings an obligation of active care. As required by the active diligence obligation, the data controller has to provide the conditions that will allow the data to be corrected. This principle, which refers to the fact that personal data must be accurate and up-to-date, is a result of the right of the person concerned to request the correction of the data.

❑ Keeping personal data in an accurate and up-to-date manner is both compatible with the interests of the data controller and also important in terms of protecting the fundamental rights and freedoms of the relevant person. In cases where the address is important in transactions, it may cause problems.

The principle of processing for certain explicit and legitimate purposes

❑ The principle of processing for certain explicit and legitimate purposes is regulated in the law in order to ensure that the relevant personal data transactions can be clearly understood by the party whose data is processed, the legal basis of the personal data processing activities is certain, the personal data processing activity and the purpose of the activity are clearly revealed. Although not explicitly stated in the law, this principle is intertwined with the principle of accountability. The purpose must be clear and legitimate.

❑ For example, it is not legitimate for an online store to process the TR ID number as data, except for the customer's name and surname, so it is against this principle. Another example of this principle is the Decision of the Personal Data Protection Board dated 27/02/2020 and numbered 2020/173. In the decision; *As a result of the application made about personal data processed by Amazon Turkey Retail Services Limited Company for the purpose of creating a member account required for shopping, accepting the "Terms of Use and Sales" and granting electronic communication permission cannot be considered as an express consent given by free will, therefore, personal data Since the principles of "compliance with the law and the rules of honesty", "**processing for specific, clear and legitimate purposes**" and "being connected, limited and proportionate to the purpose of processing" are not complied with and the data controller violates Articles 8-9 of the KVKK, It has been decided to impose an administrative fine of 1,100,000 TL within the scope of subparagraph (b) of Article (1) of Article 18 of the Law for failure to fulfill the obligations in paragraph (1) of the article.''*

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi

❑ İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, veri ekonomisi ilkesi olarak da adlandırılmakta olup amaca yetecek oranda verinin işlenmesini amaçlar. Bu ilke kişisel verilerin işlenmesinin ikincil nitelikte kalmasını, istenen amaca kişisel verilerin işlenmesinden başka bir şekilde ulaşma imkanı varsa bu yöntemin tercih edilmesi gerektiğini de vurgular. ''Ölçülülük ilkesi, veri işleme yapılmaksızın amaca ulaşmanın mümkün olmadığı hallerde kişisel veriler işlenirken gündeme gelir.'' Böyle bir sınırlamaya gidilmesinin sebebi özel hayatın gizliliği, haberleşme özgürlüğü gibi bireylerin sahip olduğu birtakım hakların ihlalini önlemektir.

❑ Danıştay'ın 11.Daire Başkanlığı 2017/816 Esas ve 2017/4906 numaralı Kararında *"davalı idarenin personellerinin yüz tanıma sistemi ile mesai kontrolünün yapılması uygulamasının personelden kişisel veri alınması kapsamında olduğu, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu açıkça görülmektedir, dava konusu işlem tarihi itibarıyla uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında, temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde ve davanın reddi yolundaki mahkeme kararında hukuka uygunluk bulunmamaktadır."* denilerek bu ilkeye atıfta bulunulmuştur.

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi

❑ İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi, varsa mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklanması gerekliliğini vurgular. Kanuni mecburiyet bulunmadığı takdirde veya verinin kullanım amacının gerçekleşmesinden itibaren kişisel verilerin yok edilmesi veya anonimleştirilmesi gerekir.

❑ Eğer kanunda ilgili verinin ne zaman yok edilmesi gerektiği hakkında bir hüküm bulunmuyorsa amaç için gerekli sürenin objektif olarak belirlenmesi gerekir. Bu belirlemeyi kişisel verileri koruma kurulu yapar. Kurulun belirlediği süreye uyulmaması halinde Türk Ceza Kanunu madde 138 gereği süreye uymayanların cezalandırılması gündeme gelir.

The principle of being relevant, limited and proportionate to the purpose

❑ The principle of being relevant, limited and proportionate to the purpose for which they are processed is also called the principle of data economy and aims to process data sufficient for the purpose. highlights. "The principle of proportionality comes to the fore when processing personal data in cases where it is not possible to reach the goal without data processing." The reason for such a restriction is to prevent violations of certain rights of individuals such as privacy of private life and freedom of communication.

❑ In the Council of State's 11th Office of the Presidency of the Decision number 2017/816 and 2017/4906, it is stated that *"the practice of controlling the personnel of the governmental administration with face recognition system is within the scope of taking personal data from the personnel and is within the scope of the principle of "privacy of private life" even in the public sphere. Considering that there is no legal basis showing the limits of the application and the principles and procedures as of the date of the action, and there is no assurance that the collected data cannot be used in any other way in the future, the action subject to the action incompatible with the fundamental rights and Constitutional principles and the court decision on the rejection of the case. There is no compliance with the law. ''* That decision is based on the principle of being relevant, limited and proportionate to the purpose.

The principle of preservation for the period stipulated in the relevant legislation or for the purpose

❑ The principle of preservation for the period stipulated in the relevant legislation or for the purpose for which they are processed emphasizes the necessity of keeping it for the period determined in the legislation or required for the purpose for which they are processed, if any. If there is no legal obligation or ıf the personal data served its purpose of use ,the data must be destroyed or anonymized.

❑ If there is no article in the law about when the data should be destroyed, the time required for the purpose must be determined objectively. This determination is made by the personal data protection board. In case of failure to comply with the time determined by the Board, punishment of those who do not comply with the time period is determined in Turkish Penal Code article 138.

İnternet Ortamında Yayınlanan İçeriklerin Kaldırılması veya Bu İçeriklere Erişimin Engellenmesi

Av.Meryem Kılıç

❑ Günümüzde teknoloji alanında yaşanan gelişmeler, kimi zaman elde edilen teknolojik güç ile bir başkasına zarar verici nitelikte fiil işlenmesine ortam hazırlayabilmektedir. Özellikle en çok rastlanılan durum bir başkasına ait olan fotoğrafın yayınlanarak bir gerçek veya tüzel kişiye maddi veya manevi zarar verilmesidir. Bu ve benzeri durumlarda yaşanılan sorunları ortadan kaldırmak için 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* yürürlüğe girmiştir.

❑ Söz konusu kanunun 1.maddesinde amaç "*içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemek*" şeklinde belirtilmiştir.

❑ Dolayısıyla internet üzerinden yayınlanan fotoğraf, haber, video benzeri istenmeyen ve hukuka aykırı içeriklere yönelik olarak içeriği kaldırma ve yayından çıkarma işlemleri yapılması bu kanun sayesinde mümkün hale gelmiştir. Özellikle kişilik haklarına aykırı nitelikte ve özel hayatın gizliliğini ihlal eden içeriklere erişimin engellenmesi hususunda yasal dayanak olarak 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun önem arz etmektedir.

İnternetten İçerik (Video, Fotoğraf, Haber, Yorum vb.) Kaldırma ve Erişimi Engelleme Halleri Nelerdir?

❑ İnternetten içerik kaldırma şartları İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun madde 8 ve 9'da sayılmıştır. Buna göre içeriğe erişimin engellenmesi şu hallerde mümkündür;

- Kişilik haklarının ihlali nedeniyle içeriğin kaldırılması veya erişimin engellenmesi,
- Suç işlenmesi nedeniyle içeriğin kaldırılması veya erişimin engellenmesi,
- Özel hayatın gizliliğinin ihlali nedeniyle içeriğin kaldırılması veya erişimin engellenmesi,

Removing or Blocking Content Published on The Internet

❑ In today's world, technological developments can sometimes provide an environment for the commitment of harmful acts to one another. The most common situation is the publication of a photograph which belongs to someone else, leading to material or moral damage to a natural or legal person. In an attempt to eliminate problems like this and many others the Law No. 5651 on *"Regulation of Broadcasts on the Internet and Fight Against Crimes Committed Through These Broadcasts"* has come into force.

❑ As stated in article 1 of the law, the purpose is "to regulate the obligations and responsibilities of content providers, host, access and collective use providers, and to regulate the principles and procedures for combating certain crimes committed on the internet via content, location and access providers".

❑ Therefore by this law, the removal of unwanted and illegal content such as photographs, news, videos published on the internet has been made possible. Law No. 5651 is of particular importance as it lays down the legal basis for access prevention to content violating the right of privacy and personal rights.

What are The Conditions for Removal Or Blocking of Content (Vıdeos, Photography, News, Comments Etc.)?

❑ The conditions in which content can be removed has been listed in articles 8 and 9 of the "Regulation of Broadcasts on the Internet and Fight Against Crimes Committed Through These Broadcasts Law";

- Removal of content or blocking of access due to violation of personal rights
- Removal of content or blocking of access due to crime,
- Removal of content or blocking of access due to violation of the right of privacy

- 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nun ihlali nedeniyle içeriğin kaldırılması veya erişim hizmetinin durdurulması,
- İnternette unutulma hakkının kullanılması nedeniyle içeriğin kaldırılması veya erişimin engellenmesi,
- Kamu yararı ve düzeni nedeniyle erişimin engellenmesi.

❑ Yukarıda sayılan hallerde, internet üzerinden yapılan yayınlar nedeniyle mağdur olan kişilerin içerik ve yer sağlayıcısına başvurarak içeriğin kaldırılmasını talep hakları vardır.

İçeriğin Kaldırılması veya İçeriğe Erişimi Engelleme Kararı Nereden Talep Edilmelidir?

Suç İşlenmesi Nedeniyle Erişimin Engellenmesi Kararını Verecek Makam

❑ Suç işlenmesi nedeniyle erişimin engellenmesi halinde, Hakim, Mahkeme veya Cumhuriyet Savcısı tarafından içeriğin kaldırılmasına veya içeriğe erişimin engellenmesine karar verilmesi mümkündür. Bu suçlar;

- İntihara yönlendirme,
- Çocukların cinsel istismarı,
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma,
- Sağlık için tehlikeli madde temini,
- Müstehcenlik,
- Fuhuş,
- Kumar oynanması için yer ve imkân sağlama suçları,
- 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.
- 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

❑ Suç işlenmesi nedeniyle erişimin engellenmesi halinde, soruşturma evresinde Sulh Ceza Hakimliği, kovuşturma evresinde ise mahkeme tarafından karar verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını 24 saat içinde hakimin onayına sunar ve hakim, kararını en geç 24 saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır.

Kişilik Haklarının İhlali Nedeniyle İçeriğin Kaldırılması veya İçeriğe Erişimin Engellenmesi Kararını Verecek Makam

❑ İnternet ortamında yapılan yayın içeriği nedeniyle, kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna

- Removal of content or blocking of access due to violation of the Law No. 5846 on Intellectual Property,
- Removal of content or blocking of access due to use of the right to be forgotten,
- Blocking of access due to public interest and public order.

❑ In the cases listed above, people who are victimized due to online broadcasts have the right to request the removal of the content by contacting the content and hosting provider.

From Whom Should The Request to Remove or Block Content be Requested?

The Authority Regarding Content Blocking Due To Crime

❑ If access is blocked due to a crime, the Judge, Court or Public Prosecutor may decide to remove the content or block access to the content. These crimes are;

- Provocation to suicide,
- Sexual abuse of children,
- Facilitating the use of drugs or stimulants,
- Supply of hazardous materials for health,
- Obscenity,
- Prostitution,
- Offenses of providing a place and opportunity for gambling,
- The crimes in the Law No. 5816 on Crimes Committed Against Atatürk, dated 25/7/1951.
- Offenses included in the Law on Betting and Chance Games in Football and Other Sports Competitions dated 29/4/1959 and numbered 7258.

❑ If access is blocked due to the commission of a crime, the decision is made by the Criminal Court of Peace during the investigation phase and by the court during the prosecution phase. During the investigation phase, in cases where delay may cause harm, the public prosecutor may decide to block access. The public prosecutor shall submit his decision to the Court within twenty-four hours and the Court shall approve the decision within twenty-four hours at the latest. If the decision is not approved within this period, the measure shall immediately be lifted by the public prosecutor.

The Authority Regarding Content Blocking Due To Personal Rights

❑ Due to the content of the broadcast on the internet, legal/natural persons and institutions/organizations claiming that their personal rights have been violated may reach out to the content provider and if unreachable, the hosting provider and request that the content be removed

ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

from the broadcast. It can also be directly requested from the Criminal Court of Peace that the content be removed and/or blocked. The requests of people claiming that their personal rights have been violated due to the broadcast content must be answered by the content and/or hosting provider within twenty-four hours at the latest.

❑ Kişilik haklarının ihlal edildiğini iddia eden gerçek veya tüzel kişi, içerik veya yer sağlayıcının talebini reddetmesi halinde veya içerik veya yer sağlayıcısına başvurmaksızın doğrudan sulh ceza hakiminden ilgili içeriğin kaldırılmasını veya içeriğe erişimin engellenmesini talep edebilir. Hâkim yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir. Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

❑ Natural/legal persons claiming that their personal rights have been violated, may request the removal or the blocking of the content directly from the Criminal Court of Peace either if the content or hosting provider refuses the request, or directly without contacting the content or hosting provider. The Court decides on the application within twenty-four hours at the latest without making a hearing. An appeal may be filed against this decision in accordance with the provisions of the Criminal Procedure Code numbered 5271. If the content subject to the blocking of access is removed from the broadcast, the decision of the Court is automatically voided.

❑ Kişilik haklarının ihlali nedeniyle içeriğin çıkarılması ve erişimin engellenmesi kararı vermeye yetkili Sulh Ceza Hakimlikleri şunlardır; İnternet sitesinin Türkiye'de bilinen bir merkez adresi varsa, bu adresteki Sulh Ceza Hakimliği içeriğin çıkarılması veya erişimin engellenmesi kararı vermeye yetkilidir. Mağdurun yerleşim yeri ve oturduğu yer Sulh Ceza Hakimliği de içeriğin çıkarılması veya erişimin engellenmesi kararı vermeye yetkilidir (5271 sayılı CMK m.12/5).

❑ For personal right violations caused online, if the website has a known address in Turkey, the Criminal Court of Peace located in that address is authorized to remove or block content. The Criminal Court of Peace located in the victim's place of residence is also authorized to decide whether the content is removed or blocked (Article 12/5 of the Code of Criminal Procedure No. 5271).

❑ Hâkim, bu kapsamda vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

❑ The Court may block content mainly by the method of blocking access to the specific content (in the form of URLs, etc.) in relation to the publication, part, section where the violation of the personality right occurred. Unless it is mandatory, it cannot be decided to block the entire broadcast on the website. However, if the Court believes that the violation cannot be prevented by blocking access to the content by specifying the URL address, he may also decide to block access to the entire publication on the website.

❑ Hâkimin verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararları doğrudan ***Erişim Sağlayıcılar Birliğine*** gönderilir. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.

❑ The decisions of the Court to remove the content and /or block access is sent directly to the ***Access Providers Association***. In case of the request of those whose personal rights are violated due to the content of the broadcast on the internet, the Court may decide not to associate the name of the applicant with the internet addresses subject to the decision. The decision shall indicate which search engines will be notified by the Union.

❑ Birlik tarafından ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcıya gönderilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği derhâl, en geç

❑ After the Union notifies the hosting or content providers, these providers must immediately or at the latest, in 4 hours take down the content. If said content

dört saat içinde ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcı tarafından yerine getirilir. Bu kapsamda hâkimin verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

❑ Sulh ceza hâkiminin kararını yukarıda belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen içerik, yer ve erişim sağlayıcıların sorumluları, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

Özel Hayatın Gizliliğini İhlal Nedeniyle İçeriğin Kaldırılması veya İçeriğe Erişimin Engellenmesi Kararını Verecek Makam

❑ İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, *Bilgi Teknolojileri ve İletişim Kurumu*'na bizzat kendileri veya avukatları vasıtasıyla doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

❑ *Bilgi Teknolojileri ve İletişim Kurumu* Başkanı, kendisine gelen bu talebi uygulanmak üzere derhâl Erişim Sağlayıcılar Birliğine bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

❑ Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar. Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

❑ Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

❑ Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. Başkan tarafından verilen erişimin

has spread to other internet addresses, the standing decision is applicable to these addresses as well.

❑ Those responsible for content, hosting and access provision who do not fulfill the decision of the Criminal Court of Peace in accordance with the conditions mentioned above and in time are punished with a judicial fine from five hundred to three thousand days.

The Authority Regarding Content Blocking Due To Violation Of The Right Of Privacy

❑ Persons who claim that their privacy is violated due to the content of broadcasting on the Internet may apply directly to the *Information and Communication Technologies Authority* themselves or through their lawyers and request the implementation of the measure to prevent access to the content. In this request; the full address (URL) of the publication that caused the right to privacy infringement, the explanation on what aspects of the right were violated and information that will prove the identity information must be included. If this information is missing, the request will not be processed.

❑ The President of the *Information Technologies and Communication Authority* immediately notifies the Access Providers Association of this request and the access providers fulfill this measure request immediately, within four hours at the latest. Blocking of access is implemented by blocking access to content (in the form of a URL) related to the publication, part, episode, image, video that violates the right to privacy.

❑ Those claiming their right to privacy was violated must present this claim to the Criminal Court of Peace within twenty-four hours of their initial request to block access to the content. The Court must then decide on the blocking of content no later than fourty-eight hours and send it directly to the Information Technologies and Communication Authority, otherwise the blocking of access will be lifted automatically. The President may appeal against this decision made by the Court in accordance with the provisions of Law No. 5271.

❑ If the content subject to the blocking of access is removed from the broadcast, the decision of the Court automatically becomes invalid.

❑ In cases where delay is harmful due to the violation of the right to privacy, the blocking of access is made by the Authority directly upon the order of the President. The decision to block access given by the President is

engellenmesi kararı, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.

Fikir ve Sanat Eserleri Kanunu'nun İhlali Nedeniyle İçeriğin Kaldırılması veya İçeriğe Erişimin Engellenmesi Kararını Verecek Makam

❑ Telif haklarının internet üzerinden ihlali halinde 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun (FSEK) Ek madde 4 düzenlemesi uygulama alanı bulur. Buna göre; hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlâlin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir.

❑ 5846 sayılı Fikir ve Sanat Eserleri Kanunu, telif haklarının ihlali nedeniyle erişimin engellenmesini değil yalnızca içeriğin kaldırılmasını kabul etmiştir. Ancak, savcılığın kararı üzerine zaten servis sağlayıcının hizmeti durdurması halinde hak ihlalinin devam etmesi engellenmiş olacaktır.

Kamu Yararı ve Düzeni Nedeniyle İçeriğin Kaldırılması veya İçeriğe Erişimin Engellenmesi Kararını Verecek Makam

❑ Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine *Bilgi Teknolojileri ve İletişim Başkanlığı* tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir. Bu kapsamda verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara Başkan tarafından elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilir.

❑ Cumhurbaşkanlığı veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar.

submitted to the approval of the Criminal Court of Peace within twenty-four hours. The Court will then announce his decision within forty-eight hours.

The Authority Regarding Content Blocking Due To Violation Of The Intellectual Property Law

❑ In case of violation of copyrights over the internet, the additional article 4 regulation of the Law No. 5846 on Intellectual Property finds application. According to this; the natural or legal person whose rights are violated first applies to the information content provider and requests that the violation be stopped within three days. If the violation continues, this time, upon the application made to the public prosecutor, within three days, the service provider is asked to stop providing service provided to the information content provider that continues with the violation.

❑ The Law on Intellectual Property No. 5846 accepted only the removal of the content, not the blocking of access due to copyright infringement. However, if the service provider stops the service upon the decision of the prosecutor, the continuation of the violation of rights will be prevented.

The Authority Regarding Content Blocking For Public Interest And Order

❑ Protection of the presidency or national security and public order, prevention of crime or at the request of the ministries concerned with the protection of general health, the *Information Technologies and Communication Department* may decide to remove the content and / or block access with regard to the publication on the internet. The decision is immediately communicated to the access providers and relevant content and hosting providers by the President. The decision to remove content and / or block access is fulfilled immediately and within four hours from the moment of notification of the decision at the latest. In this context, content and hosting providers related to access providers who fail to comply with the decision to remove the given content and / or block access are fined by the President from fifty thousand Turkish Liras to five hundred thousand Turkish Liras.

❑ The decision to remove the content and / or block access, given by the President at the request of the Presidency or the relevant Ministries, is submitted by the President to the approval of the Criminal Court of Peace within twenty-four hours. The Court announces his decision within forty-eight hours; otherwise, the decision is automatically lifted.

İşçi ile İşveren İlişkisi Bağlamında Kişisel Verilerin Korunması

Personal Data Protection in Labor Law Relations

Av.Erdem Arda Akay

Genel Olarak

❑ Son yıllarda hız kazanan teknolojik gelişmeler ışığında tüm dünyada olduğu gibi ülkemizde de sosyal ve ekonomik hayata sirayet eden kişisel verilerin korunması meselesi, hemen hemen her alanda düzenleme yapılarak kendine yer bulmuştur. Bu alanların başında da işçi-işveren ilişkisi bağlamında kişisel verilerin korunması meselesi gelmektedir.

❑ 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu ile birlikte gerçek ve tüzel kişilerin etkileşimde oldukları kişilere ait kayıt altına alınan veriler düzenlenmiştir. Bu kanun, 95/46/EC Sayılı Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Direktifi, daha sonra yayımlanarak yürülüğe giren ve direktifin yerini alan AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile 28 Ocak 1981 tarihinde Strazburg'da imzalanan 108 sayılı *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"* ile uyumlu hazırlanmış bir yasal düzenlemedir.

❑ Uluslararası Çalışma Örgütü'nün (ILO) işçilere dair kişisel verilerin işlenmesi ve bu kişisel verilere dair karşılaşılabilinecek olası kişilik haklarının ihlalini önlemeye dair bir sözleşmesi bulunmamaktadır. Ancak ILO'nun 1958 tarihli ve Türkiye tarafından 1966 yılında onaylanmış olan 111 sayılı İş ve Meslek Bakımından Ayrımcılığın Önlenmesine İlişkin Sözleşmesi, 1971 tarihli ve Türkiye tarafından 1993'te onaylanan 135 sayılı İşletmelerde İşçi Temsilcilerinin Korunması ve Onlara Sağlanacak Kolaylıklar Hakkında Sözleşmesi ile 143 sayılı tavsiye kararında, 181 sayılı Özel İstihdam Bürolarının Korunmasına İlişkin Sözleşmesinde işçilerle ilgili kişisel bilgilerin korunmasına ilişkin hükümler geliştirilmiştir. Avrupa Konseyi'nin 18 Ocak 1989'da kabul edilen İstihdam Amacıyla Kullanılan Kişisel Verilerin Korunmasına İlişkin R(89)2 sayılı Tavsiye kararı da bu konuda önemli bir kaynaktır.

❑ Bu konudaki eksikliklerin giderilmesi amacıyla ILO'nun 1995 tarih ve 267. toplantısında karar alınmış ve 1-7 Ekim 1996'da yapılan toplantılarda da çalışanların özel hayatına ilişkin bilgilerin korunması ve kullanılmasının düzenlenmesine dair bir metin geliştirilmiştir. Uluslararası Çalışma Örgütünün benimsediği ve ülkemizde de işçilerin kişisel verilerinin

Introduction

❑ Because of technological developments, the protection of personal data, which affects economic and social life, regulated in our law in almost every area as in other countries. One of these areas is labor law.

❑ With the Law on Protection of Personal Data published in the Official Newspaper on April 7, 2016 and numbered 29677, a legal framework for the protection of recorded personal data belonging to individuals with whom natural and legal persons interact. The Law on Protection of Personal Data numbered 6698 complies with General Data Protection Regulation (on April 27, 2016 and numbered 2016/679) and *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (on January 28, 1981 and numbered 108). Protection of personal data is very important in terms of privacy and general security.

❑ According to the principles adopted by the International Labor Organisation (ILO) and accepted in the context of processing personal data of workers in our country; the methods for protecting the personal data of the employees should be developed and the personal data to be processed by the data controllers should be kept to a minimum, and the personal data obtained should be limited to the areas related to the intended job.

işlenmesi bağlamında kabul edilen ilkelere göre; çalışanların kişisel veri niteliğindeki bilgilerinin korunmasına dair yöntemler geliştirilmeli ve veri sorumluları tarafından işlenecek kişisel veri düzeyi minimum seviyede tutularak, elde edilen kişisel veriler amaçlanan işe dair alanlarla sınırlı olarak kullanılmalıdır.

Veri Sorumlusu İşveren Bakımından Veri Sorumluları Siciline Kayıt Prosedürü

❑ Kişisel verilerin işlenme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişilere "veri sorumlusu" adı verilmektedir. İşveren kişi ya da kurum, kişisel verilerin işlenmesi ve korunması bağlamında veri sorumlusu unvanına sahiptir. Faaliyetleri kapsamında Türkiye'de kişisel verileri işleyen gerçek ve tüzel kişiler, kanuna göre veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilecektir.

İşveren Tarafından Yanında Çalışanlara ve Çalışan Adaylarına Ait Kişisel Veri Niteliğindeki Bilgilerin İşlenmesi

İşveren Tarafından Kişisel Verilerin İşlenmesi

❑ İşveren gerçek ve tüzel kişiler tarafından, kanun hükümlerine uymak kaydıyla çeşitli sebeplerle yanında çalışan işçilere veya çalışan adaylarına ilişkin kişisel veri niteliğindeki bilgiler toplanabilmektedir. Bu sebeplere örnek olarak işe alım sürecinde başvuran adayların değerlendirilmesi, özlük dosyası düzenlenmesi, çalışanlara yönelik terfi ve mesleki eğitim hususlarında bilgi toplanması, verilen hizmet veya üretilen ürünlere ilişkin kalite kontrol ve müşteri memnuniyetinin üst düzeyde tutulması için bilgi toplanması gösterilebilir.

❑ İşveren, iş sözleşmesi akdetmeyi düşündüğü işçi adayına ilişkin kimi özellikleri bilmek ve bu bilgiler doğrultusunda iş ilişkisine başlama kararı almak isteyebilir. Bu amaçla işçi adayına kimlik bilgilerine, yaşadığı yerin bilgisine, eğitim durumuna, daha önceki iş tecrübelerine ilişkin sorular yöneltebilir. Dikkat edilmesi gereken husus, işçiye sorularak öğrenilmek istenen bilgilerinin kapsamının yapılacak işe ve işin yürütülmesine ilişkin olmasıdır.

Data Controller Registration Procedure for Employers

❑ The data controller is the natural or legal person who determines the purposes and tools of processing personal data and is responsible for the creation and management of the filing system. The employer person or institution has the title of data controller in the context of processing and protection of personal data. Natural or legal person employers who process personal data shall register with the Data Controllers Registry prior to commencing processing. However, considering objective criteria that shall be designated by the Board such as the characteristics and the number of data to be processed, whether or not data processing is based on any law, or whether data will be transferred to third parties, the Board may set forth exemptions to the obligation to register with the Data Controllers Registry.

Processing of Personal Data Information about Employees and Candidates

Processing of Personal Data by the Employer

❑ Employers can collect personal data on job applicants and employees for a number of purposes. Examples of these reasons are the evaluation of applicants, the preparation of a personal file, the collection of information on promotion and training for employees, and ensure personal safety, personal security, quality control, customer service and the protection of property.

❑ The employer may want to know some features related to the candidate for employment, and he intends to decide accordingly. For this, the employer can ask prospective employees about their identity information, knowledge of their place of residence, educational status, and previous work experience. It should be noted that the scope of the information to be learned is related to the job.

❑ Employee identification information, professional success, continuity and efficiency can be collected by the employer in the form of personal data to be used later on in business. The point to be considered here is that this data is used with the explicit consent of the worker or in exceptional cases, even if consent is not required, in accordance with the good faith. Sharing such personal data will only be possible if third parties have a fair interest.

İşverenin Kişisel Verilerin Korunması Bağlamındaki Yükümlülükleri

Türk Borçlar Kanunu bağlamında;

❑ Yürütülen iş ilişkisi çerçevesinde işçinin kişisel veri niteliğindeki bilgileri, işveren tarafından işlenecek ve gerekli işlemlerde bu verilerden yararlanılabilecektir. Ancak işçinin iş sözleşmesinden dolayı işverene karşı belirli yükümlülükleri olduğu gibi işverenin de işçiye karşı sözleşmeyle yükümlülük altına girdiği hususlar mevcuttur. İşverenin bu yükümlülüklerinden biri de işçiyi gözetme yükümlülüğüdür.

❑ Bu bağlamda 6098 sayılı Türk Borçlar Kanunu'nun 419. maddesinde "İşçinin kişiliğinin korunması" başlığı altında işçilere ait kişisel verilerin kullanılması konusu düzenlenmiştir.

> ***"Kişisel verilerin kullanılmasında***
> ***MADDE 419- İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.***
> ***Özel kanun hükümleri saklıdır."***

❑ İlgili TBK hükmü iş hukuku bağlamında düzenlenen iş sözleşmeleri açısından geçerlidir ve veri sorumlusu işveren tarafından kişisel verilerin işlenmesi ve kullanılması işlemi buna uygun yürütülecektir. İşçinin işe yatkınlığı veya hizmet sözleşmesinin ifası için zorunlu olmadığı sürece işçinin kişisel veri niteliğindeki bilgileri kullanılamayacaktır.

İş Kanunu Bağlamında;

❑ İşveren, iş sözleşmesi ile yanında çalışan işçilerin kişisel veri niteliğindeki bilgilerini de mevzuata uygun şekilde işlemek ve korumak durumundadır. İşçilerin, işveren tarafından işlenen kişisel verilerine dair en tipik örnek işçi özlük dosyasıdır. 4857 sayılı İş Kanunu'nun 75. maddesinde işçi özlük dosyasına işlenmek adına işveren tarafından elde edilen bilgilerin kullanımı ve korunması konusu işlenmiştir:

> ***"İşçi özlük dosyası***
>
> ***Madde 75 - İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.***
> ***İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."***

Employer's Obligations in the Context of Protection of Personal Data

In the Context of Turkish Law of Obligations:

❑ The personal data of the employee in the labor relationship will be processed by the employer and this data can be used when necessary. However, as the employee has certain obligations to the employer due to the employment contract, there are also issues where the employer is under obligation with the contract against the employees. One of them is the obligation of protect the employee.

❑ In this context, the subject of using personal data of employees is regulated under the title of "Protection of the employee's personality" in the article 419 of the Turkish Code of Obligations numbered 6098:

> ***"In the use of personal data***
> ***ARTICLE 419- The employer may use the personal data of the employee only to the extent that it is related to the worker's predisposition or is necessary for the performance of the service contract.***
> ***Special law provisions are reserved."***

❑ The relevant law provision is valid in terms of employment contracts arranged in the context of labor law, and the processing and use of personal data by the data controller employer will be carried out accordingly. The employee's personal data won't be used unless it is mandatory for the employee's ability to work or the performance of the service contract.

In the Context of Labor Law;

❑ The employer is obliged to process and protect the personal data of the employees who are working with the employment contract in accordance with the legislation. The most typical example of employees personal data processed by the employer is the employee personal file. In the 75th article of the Labor Law numbered 4857, the issue of the use and protection of the information obtained by the employer to be processed in the employee personal file is discussed:

> ***ARTICLE 75. – The employer shall arrange a personal file for each employee working in his establishment. In addition to the information about the employee's identity, the employer is obliged to keep all the documents and records which he has to arrange in accordance with this Act and other legislation and to show them to authorised persons and authorities when requested.***
> ***The employer is under the obligation to use the information he has obtained about the employee in congruence with the principles of honesty and law and not to disclose the information for which the employee has a justifiable interest in keeping as a secret.***

❑ İşçinin kimlik bilgileri, mesleki başarısı, devamlılığı ve verimliliği gibi konularda işveren tarafından kişisel veri niteliğindeki bilgiler daha sonra iş ile alakalı kullanılmak üzere toplanabilecektir. Burada dikkat edilmesi gereken nokta, bu verilen işçinin rızasıyla veya istisna hallerde rıza aranmasa dahi dürüstlük kurallarına uygun olarak toplanması ve kullanılmasıdır. Söz konusu kişisel verilerin paylaşılması, ancak 3. kişilerin haklı menfaati olması halinde mümkün olabilecektir.

❑ İş Kanunu'nun 25. maddesinde ise işverenin haklı nedenle derhal fesih hakkı düzenlenmiştir. İlgili maddede; işçinin tutulduğu hastalığın tedavi edilemeyecek nitelikte olduğu ve işyerinde çalışmasında sakınca bulunduğunun saptanması durumunda veya işçinin kendi kastından veya derli toplu olmayan yaşantısından yahut içkiye düşkünlüğünden doğacak bir hastalığa ya da engelli duruma düşmesi nedeniyle oluşan devamsızlığında işverenin sözleşmeyi haklı nedenle derhal feshedebileceği belirtilmiştir. Bu madde kapsamında işverenin, işçinin sağlık verilerine amaca yönelik olarak ulaşma hakkının bulunduğu görülmektedir. Bununla birlikte yine aynı madde uyarınca; işçinin iş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri için gerekli vasıflar veya şartlar kendisinde bulunmadığı halde bunların kendisinde bulunduğunu ileri sürerek ya da gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işvereni yanıltması durumunda da işverenin haklı fesih olduğunun belirtilmesi, işverenin işe almadan önce işçiyle yapacağı görüşmelerde sözleşmenin esaslı konularına ve işçinin temel özelliklerine ilişkin hususlarda kişisel veri niteliğinde bilgileri talep edebileceğini göstermektedir.

İş Sağlığı ve Güvenliği Kanunu ve yönetmeliği bağlamında;

❑ İşçinin sağlık bilgileri, Kişisel Verilerin Korunması Kanunu 6. madde bağlamında özel nitelikli kişisel veriler arasında sayılmıştır. Kanun özel nitelikteki kişisel verilerin işlenebilmesi için açık rızayı şart koşmuş ancak ilgili maddenin devamında sağlık ve cinsel hayata ilişkin verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla işlenebileceğini şerh düşmüştür. Bu bağlamda hassas veri olarak da nitelendirilen özel nitelikli kişisel verilerin hukuka uygun işlenmesi veri sorumluları açısından büyük önem arz etmektedir.

❑ Bilindiği gibi kişisel verilerin işlenmesi kavramı üst başlık olarak bu verilerin aktarılması, saklanması, korunması ve yok edilmesi gibi birçok veri işlemini kapsamaktadır. 6331 sayılı İş Sağlığı ve Güvenliği Kanununu da, işçinin kişisel veri kapsamındaki sağlık bilgilerinin gizli tutulması konusunda işverene yükümlülük getirilmiştir. İlgili kanunun ***"Sağlık Gözetimi"***

❑ Information in the nature of personal data by the employer on matters such as the employee's identity information, professional success, continuity and productivity can be collected for later use in relation to the job. The point to be considered here is that this employee is collected and used in accordance with the rules of honesty, even if consent is not sought in exceptional cases. Sharing the personal data in question will only be possible if there is a legitimate interest of third parties.

❑ In the 25th article of the Labor Law, breaking of the employment contract by the initiative of the employer is regulated. In the relevant article; it has been stated that the employer may terminate the contract immediately for a justified reason, if the disease in which the employee is detained is incurable and it is determined that there is a harm in working at the workplace, or if the employee is absent due to a disease or disability arising from his own intentions or unclear life or addiction to alcohol. With the scope of this article, it is seen that the employer has the right to access the health data of the employee for the purpose. However, in accordance with the same article stating that the employer is justified termination, even if the employee misleads the employer by claiming that he / she does not have the qualifications or conditions required for one of the essential points of this contract at the time of the employment contract, or by saying that he / she doesn't have them, or by saying untrue information or words, It shows that it may request information in the nature of personal data regarding its fundamental issues and basic characteristics of the employee.

In the Context of Occupational Health and Safety Law and regulations:

❑ The health information of the employee has been counted among the special categories of personal data in the context of Article 6 of the Protection of Personal Data Law. The law stipulates explicit consent for the processing of personal data of special nature, but it is stated that the data related to health and sexual life can be processed for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing. In this context, the legal processing of special categories of personal data, which is also considered as "special categories of personal data", is of great importance for data controllers.

❑ The concept of processing personal data covers many data operations such as transferring, storing, protecting and destroying these data. In the Occupational Health and Safety Law No. 6331, the employer is obliged to keep the health information of the employee confidential. In accordance with the last paragraph of the 15th article of the relevant law titled ***"Health Surveillance"***, the

başlıklı 15. maddesinin son bendi uyarınca işveren, sağlık muayenesi yaptırılan çalışanın özel hayatı ve itibarının korunması açısından sağlık bilgilerini gizli tutmakla yükümlüdür.

❑ Kanuna paralel olarak hazırlanan İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği de işverene, iş sağlığı ve güvenliği faaliyetlerine ilişkin kaydı ve işçilerin kişisel sağlık dosyalarını saklama yükümlülüğü getirmiştir. İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği'nin 7. Maddesi uyarınca işveren, ilgili mevzuatta belirlenen süreler saklı kalmak kaydıyla; işyerinde yürütülen iş sağlığı ve güvenliği faaliyetlerine ilişkin her türlü kaydı, işten ayrılma tarihinden itibaren en az 15 yıl süreyle çalışanların kişisel sağlık dosyalarını saklamakla yükümlüdür.

❑ Bununla birlikte işçinin işyerinden ayrılarak başka bir işyerinde çalışmaya başlaması halinde, yeni işveren çalışanın kişisel sağlık dosyasını yazılı olarak talep edecek, önceki işveren dosyanın bir örneğini onaylayarak bir ay içerisinde yeni işverene gönderecektir. Onaylı defterin asıl suretini işveren, diğer suretlerini ise iş güvenliği uzmanı ve işyeri hekimi saklama yükümlülüğü altındadır. Defterin imzalanması ve düzenli tutulmasından işveren sorumludur ve olası bir teftiş durumunda yetkili iş müfettişleri her istediğinde işveren onaylı defteri göstermek zorundadır.

Veri sorumlusu işverenin, yanında çalışan işçinin kişisel veri niteliğindeki bilgilerini işlerken uyması gereken bazı yükümlülükler bulunmaktadır:

Aydınlatma yükümlülüğü ve açık rıza alınması;

❑ İlgili kişiye ait kişisel verilerin işlenebilmesi, istisnai haller saklı kalmak üzere açık rızaya bağlıdır. Ancak bu açık rızanın varlığı halinde veri işleme ve saklama prosedürleri uygulamaya konabilecektir. Kanunda açık rıza kavramı; belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza olarak ifade edilmiştir. Söz konusu bilgilendirme de KVKK m.10 uyarınca düzenlenmiş aydınlatma yükümlülüğü çerçevesinde gerçekleştirilecektir. Hem iş başvurusunda bulunan kişilerin hem de işveren yanında çalışan işçilerin kişisel verilerinin ne amaçla işlendiği, nerede depolandığı, kimlerle paylaşılabileceği gibi hususlarda veri işlenme sürecine başlamadan bilgilendirilmesi gerekmektedir.

Verilerin belirtilen amaçlarla ve sürelerle sınırlı olarak kullanılması;

❑ Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesiyle getirilen prensibe göre işverenin, yalnızca yapılan iş bakımından elzem ve işin yürütülmesiyle ilgili verileri işlemesi esas tutulmuştur. İşveren, aydınlatma

employer is obliged to keep the health information confidential in order to protect the private life and reputation of the employee who was examined.

❑ In addition, with the regulation, the employer is obliged to keep the records of occupational health and safety activities and the personal health files of the employees. Without other periods specified in the relevant legislation, the employer is obliged to keep all kinds of records regarding occupational health and safety activities carried out in the workplace, and personal health files of employees for at least 15 years from the date of resignation.

❑ On the other hand, if the employee leaves the workplace and starts working in another workplace, the new employer will request the employee's personal health file in writing, the previous employer will approve a copy of the file and send it to the new employer within a month. The employer is under the obligation to keep the original copy of the approved book, and the occupational safety specialist and the workplace doctor in other copies. The employer is responsible for signing and keeping the ledger in order, and in case of a possible inspection, the employer must present the approved book whenever the authorized labor inspectors request.

❑ There are some obligations that the data controller employer must comply with while processing the personal data of the employee working with her/him:

Obligation to Inform and Explicit Consent;

❑ Explicit consent is defined as freely given and informed consent. Explicit consent of the person concerned is required to process personal data, with exceptions. Data processing will only be possible if this explicit consent exists. The consent of the person concerned should be given at the end of an information process. This information will also be carried out in accordance with the obligation to inform regulated in accordance with Art. 10 in Protection of Personal Data numbered 6698.

Limited use of data for specified purposes and times;

❑ According to the principle adopted in the Law on Protection of Personal Data, the employer is only required to process data essential for the work performed and the execution of the work. The employer will be able to use the personal data of the worker, which he informs in the context of the obligation to inform, in this information, for the purpose and time limited to the worker.

yükümlülüğü bağlamında bilgilendirdiği işçinin kişisel verilerini, bu bilgilendirmede işçiye aktarılan amaçla ve süreyle sınırlı olarak kullanabilecektir.

Verilerin kanuna uygun olarak üçüncü kişilere aktarılması;

❑ Kişisel Verilerin Korunması Kanunu'nun 8. maddesinde düzenlenen verilerin aktarılması hususu, kural olarak ilgili kişinin açık rızasına bağlanmıştır. Kanundan belirtilen ilkeler çerçevesinde işlenmek amacı ile elde edilen kişisel veriler ilgili kişinin açık rızası alınmak sureti ile Türkiye'de üçüncü kişilere aktarılabilecektir. Ancak Kanun'un 5.maddesinin 2.fıkrasında ve yeterli önlemler alınmak kaydıyla 6.maddesinin 3.fıkrasındaki şartlardan birinin mevcut olması durumunda işçinin açık rızası aranmaksızın veri sorumlusu işveren tarafından kişisel verilerin aktarımı gerçekleştirilebilecektir.

Verilerin güvenliğinin sağlanması;

❑ Veri sorumlusu işveren, aynı zamanda veri sistemine işlenen bu kişisel veri niteliğindeki bilgilerin korunmasından da sorumludur. KVKK m. 12'de veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini engellemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü tedbiri alması gerektiği belirtilmiştir.

Veri Sorumlusu İşveren Tarafından Kişisel Verilerin İşlenmesi ve Korunmasına Dair Yürütülecek Politikanın Belirlenmesi

❑ Mevzuata uygun bir şekilde kişisel verileri işleyen ve bunları veri sisteminde depolayan veri sorumlusu işveren, aynı zamanda bünyesindeki kişisel verilerin güvenliğinden de sorumlu olacaktır. Kanunun 12. maddesinde veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu belirtilmiştir.

❑ Bu kapsamda işverenlerin, teknik ve hukuki destek ile güvenlik prosedürü geliştirmesi işçilerin kişisel verilerinin korunmasına ilişkin olası risklerin önüne geçilmesini sağlayabilecektir. İdari ve hukuki anlamda; mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları uygulanması ve kişisel verilerin mümkün olduğunca azaltılması gibi tedbirlere başvurulabilecektir. Teknik anlamda ise siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel verilerin bulutta depolanması gibi tedbirler alınarak kişisel verilerin korunması sağlanabilecektir.

Transferring data to third parties in accordance with the law;

❑ According to Article 8 of the Personal Data Protection Law, the issue of transferring data is subject to the explicit consent of the person concerned. Personal data shall not be transferred without obtaining the explicit consent of the data subject. But personal data may be transferred without obtaining the explicit consent of the data subject if one of the conditions set forth under the following exists the second paragraph of article 5 and on the condition that adequate measures are taken, the third paragraph of article 6.

Protect the personal data;

❑ The employer is also responsible for the protection of this personal data information entered into the data system. The employer should take all necessary technical and organisational measures to prevent the illegal processing of personal data, to prevent illegal access to personal data and to ensure the protection of personal data.

Policy Determination by the Employer on the Processing and Protection of Personal Data

❑ The employer will also be responsible for the security of personal data. In accordance with Article 12 in the Law, data controller to prevent personal data from being processed illegally, to prevent personal data from being accessed illegally and to take all necessary technical and administrative measures to ensure the appropriate level of security to ensure the retention of personal data. In this context, the development of security procedures with technical and legal assistance will prevent data risks.

İşveren Tarafından Kişisel Verilerin Korunması Kanunu'na Uygun Hareket Edilmemesi Durumunda Karşılaşılabilecek Yaptırımlar

❑ Kişisel verilerin mevzuat hükümlerine göre işlenmemesi veya hukuka aykırı bir sonucun ortaya çıkarılması halinde veri sorumlularının karşı karşıya kalacağı müeyyideler 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 17. ve 18. maddelerinde gösterilmiştir.

❑ 6698 sayılı Kanun'un 17.maddesi "Suçlar" başlığı altında TCK'nın 135 ila 140. maddelerine atıf yapmış ve cezai yönden veri sorumlularının kişisel verilerin kaydedilmesi, verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi, verileri yok etmeme suçlarına ilişkin sorumlu olacakları belirtilmiştir. Bununla birlikte Kişisel Verilerin Korunması Kanunu'nun 7. maddesinde düzenlenen "kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" kurallarına aykırı hareket edenlerin TCK m.138 kapsamında cezalandırılacağı ortaya konmuştur.

❑ 6698 sayılı Kanun'un 18.maddesinde ise "Kabahatler" başlığı altında; aydınlatma ve veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi, Kişisel Verilerin Korunması Kurulu tarafından verilen kararların yerine getirilmemesi ve veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi hallerinde veri sorumlarına ilişkin idari para cezası öngörülmüştür. Söz konusu idari para cezaları, hem gerçek kişi hem de tüzel kişi veri sorumluları hakkında uygulanacaktır. İdari para cezasına hükmetme yetkisi Kişisel Verilerin Korunması Kurulu'na aittir. Kurul, veri sorumlusunun mali durumu ve ihlalin niteliğine göre kanunda belirtilen aralıkta bir cezaya hükmedecektir. Buna ek olarak veri sahibinin bir zarara uğraması halinde tazminat talep etme hakkı da saklıdır.

Sanctions in the Law on Protection of Personal Data Against Employers

❑ If personal data are not processed in accordance with the provisions of the legislation or if an unlawful result is found, the sanctions that the data controllers will face are shown in the 17th and 18th articles of the Personal Data Protection Law No. 6698.

❑ In the 17th article of the Law No. 6698, under the title of "Crimes"; data controllers are responsible for the recording of personal data, the illegal delivery or capture of data, crimes not to destroy the data in crime terms.

❑ In the 18th article of the Law No. 6698, under the title of "Misdemeanors"; data controllers will be responsible and will be punished with administrative fines if they don't fulfil obligation to inform stipulated in article 10 of this Law, obligations regarding data security stipulated in article 12 of this Law, decisions of the Board as per article 15 of this Law and obligation to register with the Data Controllers Registry and notification stipulated by article 16 of this Law. Administrative fines envisaged by this article shall apply to natural persons and private law legal persons who are data controllers. The Board will rule a penalty in the range specified in the law, based on the financial status of the data controller and the nature of the violation. In addition, the data subject can claim compensation in case of personal damage.

Tüzel Kişilerin (Anonim Şirket, Limited Şirket ve Diğer Şahıs Şirketlerinin) Veri Sorumluları Sicili'ne (VERBİS'e) Kayıt Süreci

The Enrollment Process of Legal Persons (Corporations, Limited Companies and Partnerships) to the Data Controllers Registry (VERBIS)

Av.Meryem Kılıç
Av.Ayşe Hüma Lofça

❑ 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 16'da yer alan düzenleme ile kişisel veri işleyen tüzel kişi (Anonim şirket, limited şirket ve diğer şahıs şirketleri) veri sorumlularının kişisel veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolması zorunlu tutulmuştur. Kural Sicil'e kaydolmayı öngörse de bu Sicil'e kaydolmaktan muaf tutulanlar da vardır. Bu konuya aşağıda ayrıntıları ile değinilecektir.

❑ Aşağıda açıklanacağı üzere Sicil'e kaydolmaktan muaf tutulanlar dışındakiler için yasal zorunluluk gereği Sicil'e kişisel veriler işlenmeye başlanmadan önce kayıt olunması esastır. Bu nedenle tüzel kişilerin VERBİS sistemine kayıt sürecinin incelemesinin faydalı olacağı düşünüldüğünden, yazımızda öncelikle Sicil'e kayıt olmaktan muaf tutulanlar ve devamında da muaf tutulmayanlar için kayıt süreci irdelenecektir.

Veri Sorumluları Sicili'ne Kaydolmaktan Muaf Tutulanlar

❑ Kişisel Verileri Koruma Kanunu madde 16'da genel hatlarını belirleyerek kurula Sicil'e kayıttan muaf tutulacak kişileri belirlemede hareket alanı tanımıştır. Kurul da anılan yasal düzenlemenin verdiği takdir yetkisini kullanarak Sicile kayıt yükümlülüğüne istisna getirilen veri sorumluları ile ilgili 02.04.2018 tarihli ve 2018/32 sayılı kararı ile aşağıdaki kişileri Sicil'e kaydolmaktan muaf tutmuştur. Bunlar;

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,
- Noterler,
- Yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye'de yerleşik dernek, vakıf ve sendikalar,
- Siyasi partiler,
- Avukatlar,
- Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler.

❑ Ayrıca yukarıda sayılanlar dışında Kişisel Verileri Koruma Kurulu; kişisel verinin niteliği, kişisel verinin sayısı, kişisel verinin işlenme amacı, kişisel verinin işlendiği faaliyet alanı, kişisel verinin üçüncü kişilere

❑ According to article 16 of the 6698 numbered Law on the Protection of Personal Data, legal persons who process personal data are required to enroll in the Registry of Data Controllers before proceeding with data processing. Although registration is foreseen, some legal persons are held exempt from this rule. This topic will be discussed in detail below.

❑ As it will be explained below, those who are not exempt from registration are under legal obligation to enroll in the Registry of Data Controllers before beginning data processing. For this reason the examination of the enrollment process of legal persons is useful and will be done in the order of exceptions and non-exceptions.

Exceptions to the Data Controllers Registry (VERBIS)

❑ Article 16 of the Personal Data Protection Law has generally outlined those under obligation to register; leaving room for the Board to interpret those who are exempt. The Board, using its discretion power, has listed these exceptions to enrollment in its 02.04.2018 dated and 2018/32 numbered decision as shown below;

- Those who, while are a part of a registration data segment but process personal data only by non-automatic means.
- Notaries
- Organizations, foundations and unions whom process data limited only with their field of activity and only in accordance with the related legislation and purposes.
- Political Parties,
- Attorneys at Law and Legal Advisers,
- Independent Accountant Financial Advisers and Sworn-in Public Accountants.

❑ In addition to the list above, the Data Protection Board may determine exceptions based on criterias such as the nature of the personal data, the quantity of personal data, the purpose of processing the personal data, the field of practice in which the personal data has been processed,

aktarılma durumu, kişisel veri işleme faaliyetinin kanunlardan kaynaklanması, kişisel verilerin muhafaza edilmesi süresi, veri konusu kişi grubu veya veri kategorileri kriterlerine göre Sicil'e kayıttan muaf tutulacak veri sorumlularını belirleyebilir. Kurul bu kriterlere göre belirlediği istisnaları uygun usulle kamuoyuna duyurur.

Veri Sorumluları Sicili'ne Kayıt Süreci Hakkında Genel Bilgi

❑ Öncelikle belirtmekte fayda vardır ki VERBİS'e kayıt sadece internet üzerinden yapılabilmekte olup yazılı olarak başvuru yapılması mümkün değildir. VERBİS'e kayıt için "Yurtiçinde Yerleşik Tüzel Kişi, Yurtdışında Yerleşik Tüzel Kişi, Kamu Kurum ve Kuruluşları" olmak üzere üç farklı seçenek bulunmaktadır. Türkiye'de yerleşik olan veri sorumluları doğrudan, Türkiye'de yerleşik olmayan veri sorumluları ise ancak yetkilendirecekleri temsilcisi vasıtasıyla Sicil'e kayıt olabilirler.

Veri Sorumluları Sicili'ne Kayıt Sırasında İzlenmesi Gereken Adımlar

❑ Kişisel Verileri Koruma Kurumunun web sitesine (www.kvkk.gov.tr) giriş yapılır.

❑ Sitede sağ tarafta yer alan **VERBİS** butonuna tıklanarak kayda başlanmış olunur.

❑ İlk olarak sisteme kayıt olunması gereklidir. Web sitesine girişte "Veri Sorumlusu Yöneticisi Girişi" butonuna tıklanarak akabinde gelen "Kayıt Olun" butonuna tıklanır.

❑ Karşımıza çıkan ekranda kayıt için uygun seçenek seçilir. (Yukarıda da bahsedildiği üzere VERBİS'e kayıt için "Yurtiçinde Yerleşik Gerçek / Tüzel Kişi, Yurtdışında Yerleşik Gerçek / Tüzel Kişi, Kamu Kurum ve Kuruluşları" olmak üzere üç farklı seçenek bulunmaktadır.) Bu başvuruyu kategorilere göre "Veri sorumlusu yöneticisi ya da veri sorumlusu temsilcisi veya kamu kurumlarınca belirlenen koordinasyon görevlisi istenen bilgileri girerek başvuru formunu ıslak imzalı şekilde kuruma iletilerek yapar. Ya da kep adresinden Kurumun kep adresine göndermek yeterli olmaktadır.

❑ Kayıt esnasında Veri Sorumlusunun aşağıdaki bilgilerine ihtiyaç duyulur;

- Kimlik ve adres bilgileri,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,

the status of data transfer to third parties, the legal basis of personal data processing, the retention span of the data and the data subject or category. The Board announces these criteria to the public with the appropriate procedure.

General Information About The Registry Of Data Protection

❑ It should be pointed out that enrollment may only be done online, written applications are not accepted. There are three application categories at VERBİS; Legal Person Residing in Turkey, Legal Person Residing Abroad, Public Institutions and Organizations. Legal persons residing in Turkey may apply directly while legal persons residing abroad may only apply through an authorized representative.

Steps to Follow While Registering to VERBİS

❑ Enter the Personal Data Protection Authority website(www.kvkk.gov.tr).

❑ Click the VERBİS button on the top left. Scroll down and click "For VERBİS' Page". Please note that the application must be done in Turkish.

❑ Select the **"Veri Sorumlusu Yönetici Girişi"** button. This will direct you to the controller entry. Choose the register button, "Kayıt olun".

❑ Next you will be directed three options; Yurtiçinde Yerleşik Tüzel / Gerçek Kişi (Legal / Natural Person Residing in Turkey), Yurtdışında Yerleşik Tüzel / Gerçek Kişi (Legal/ Natural Person Residing Abroad), Kamu Kurumu (Public Establishment). Please select your corresponding status. According to your status, the necessary information will be filled out with the title controller, authorized representative or coordination officer determined by public establishments. This form will be signed with a wet signature or with a KEP address (a registered electronic mail address) and sent to the Board.

❑ During registration, the following information of the Data Controller is required;

- Identification and address information,
- The purpose of data processing,
- The group or groups subject to data processing and statements about these persons' data categories,
- Recipient or recipient groups to which the personal data may be transferred,

- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Kişisel veri güvenliğine ilişkin alınan tedbirler,
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre,
- Varsa KEP (Kayıtlı Elektronik Posta) Adresi.

❑ Veri sorumlularının yukarıda yer verilen bilgileri sistemde doldurduktan sonra oluşturdukları başvuru formunu Kuruma kargo / posta / elden iletilmesi veya Kayıtlı Elektronik Posta (KEP) aracılığıyla iletmesi gerekmektedir.

Veri Sorumlularının Kayıt Sürecini Tamamladıktan Sonraki Bildirim Yükümlülüğü

❑ Veri Sorumlularının Veri Sorumluları Sicili'ne kaydolduktan sonra, Kurum tarafından kendilerine iletilen "kullanıcı adı" ve "parola" ile VERBİS'e giriş yaparak bildirim yapması gerekmektedir.

Veri Sorumluları Sicili'ne Kayıt Süresi

❑ Önemle belirtmekte fayda vardır ki 30 Eylül 2020 tarihine kadar Sicile kayıt yükümlülüklerini yerine getirmesi gereken veri sorumlularının; fiili, teknik ya da hukuki imkânsızlık nedeniyle Sicile kayıt yükümlülüğünü yerine getiremediği göz önüne alınarak, Kurul tarafından, birer yazı ile kayıt yükümlülüğünü yerine getirmeleri için süre tanımıştır. Söz konusu yazıyla Kurul tarafından kendilerine bildirilen süre içerisinde, ilgili veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri gerekmektedir.*(Kurulun 01.10.2020 tarihli ve 2020/760 sayılı kararı)*

- Personal data which may be transferred to foreign countries,
- Precautions taken regarding personal data protection,
- The maximum time period required to process the data according to the purpose,
- If available, a KEP address (registered electronic mail address).

❑ After filling out the information above, the controllers must deliver the form either by shipping, hand delivery or with the KEP address.

The Data Controllers' Notification Duty After Completing The Registration Process

❑ The controllers must login to VERBİS using the "username" and "password" provided by the Board and reports their registration.

The Registration Period to the Data Controllers Registry VERBIS

❑ It is highly important to point out that if those who must have been registered by 30.09.2020 weren't able to fulfill their registration obligation due to actual, technical or legal impossibilities, the Board has given time to fulfill the registration obligation with a letter. Within the period notified to them by the Board in said letter, the data controllers are required to fulfill their registration obligation to the Registry. *(Board's decision dated 01.10.2020 and numbered 2020/760)*

	Veri Sorumluları (Data Controllers)	Kayıt Yükümlülüğünün Başlama Tarihi (Start Date of Registration Obligation)	Önceki Son Tarih (First Last Date)	Güncel Son Tarih (Updated Last Date)
1	Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan veri sorumluları Data controllers with more than 50 employees or an annual financial balance of more than 25 million TL	01.10.2018	30.06.2020	30.09.2020
2	Yurtdışında yerleşik veri sorumluları Data controllers residing abroad	01.10.2018	30.06.2020	30.09.2020
3	Yıllık çalışan sayısı 50'den az veya yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan veri sorumluları Data controllers with less than 50 employees or an annual financial balance of less than 25 million TL whose main activity is the processing of "special categories of personal data"	01.01.2019	30.09.2020	31.03.2021
4	Kamu kurum ve kuruluşu olan veri sorumluları Data controllers who are public establishments and organizations	01.04.2019	31.12.2020	31.03.2021

Veri Sorumluları Sicili'ne Kaydolmamanın Yaptırımı

❑ Kişisel Verileri Koruma Kanunu'nun 18. maddesi uyarınca VERBİS'e kayıt ve bildirim yükümlülüğünü yerine getirmeyen veri sorumluları hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası uygulanabilecektir. Dolayısıyla ilgili veri sorumlularının bu yaptırım ile karşılaşmamaları için yukarıda öngörülen tarihlere kadar VERBİS kayıtlarını tamamlamaları gerekmektedir.

Veri Sorumluları Sicili'ndeki Bilgilerde Değişiklik Olması

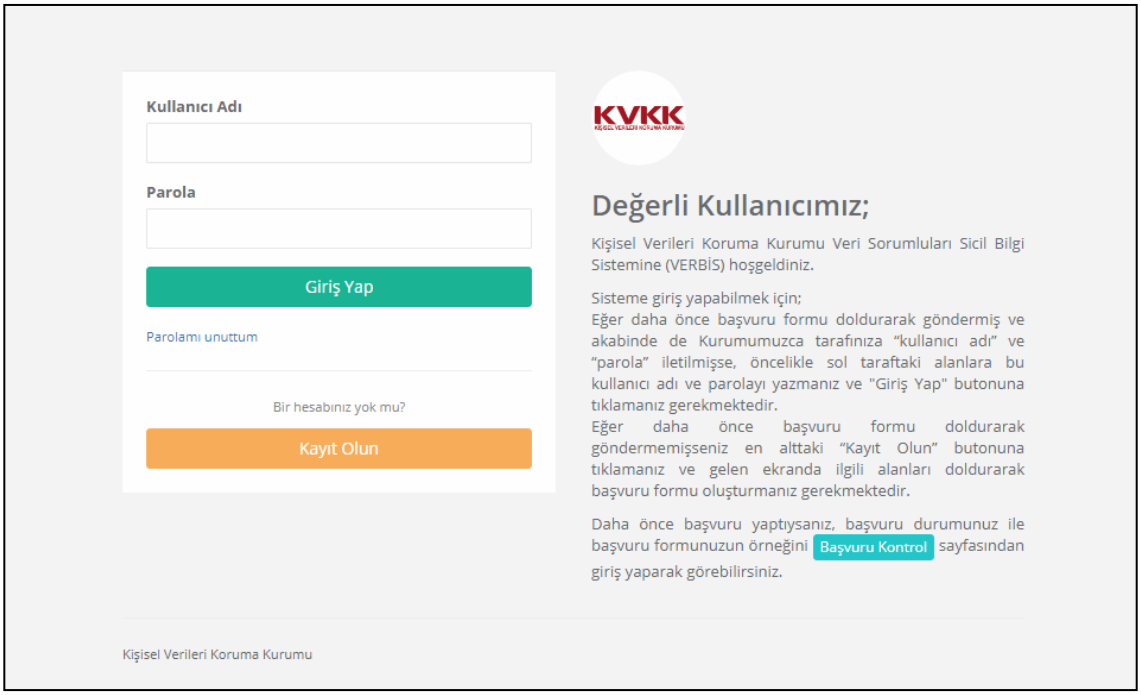
❑ Veri Sorumlusunun Sicil'de kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden Kuruma bildirmesi gereklidir.

Enforcement Of Non-registration to The Data Controllers Registry (VERBIS)

❑ Article 18 of Law on the Protection of Personal Data states that Administrative fines from 20,000 TL to 1,000,000 TL may be imposed on data controllers who fail to fulfill their obligation to register and notify VERBIS. Therefore, in order to avoid this sanction, the relevant data controllers must complete their VERBIS records until the dates shown above.

Change Of Information in the Data Controllers Registry

❑ Any change that may occur must be reported to the Board through VERBİS within seven days of the change.



Yurtdışında Yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü'ne dair Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Kararının İncelenmesi

Review of Decision Dated 23.07.2019 and Numbered 2019/225 Issued by The Personal Data Protection Board

Av.Erdem Arda Akay

❑ Kişisel Verilerin Korunması Kurulu tarafından verilen 23.07.2019 tarih ve 2019/225 sayılı karar ile Türkiye'de doğrudan veya şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunan yurt dışında yerleşik veri sorumlularının Sicile kayıt olmaları gerektiği belirtilmiş; buna karşın Türkiye'de ticari faaliyette bulunmayan ve yalnızca haberleşme, tanıtım, reklam ve şirkete bilgi verme gibi amaçlarla açılan irtibat bürolarının veri sorumluları siciline kayıt yükümlülüklerinin olmadığına hükmedilmiştir.

With the Decision dated 23.07.2019 and numbered 2019/225 issued by the Personal Data Protection Board, located directly abroad or companies with branches in Turkey should be noted the Registry Records; on the other hand, liaison offices which don't do any commercial activities in Turkey but only working for the purposes of communication, promotion, advertisement and providing information to the company, don't have an obligation to register the data controllers registry.

Karar Özeti

Kişisel Verilerin Korunması Kurulu, kendisinden görüş talebinde bulunulması üzerine verdiği kararda;

"a) Türkiye'de doğrudan veya şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunan yurt dışında yerleşik veri sorumlularının Sicile kayıt olmalarının gerektiğine,

b) Yurt dışında yerleşik tüzel kişilerin Türkiye'deki şubelerinin, Kanunda yer alan veri sorumlusu tanımı gereği kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemesi ve veri kayıt sisteminin kurulması ile yönetilmesinden sorumlu olması halinde yurt dışında yerleşik tüzel kişiden ayrı olarak Türkiye'de yerleşik veri sorumlusu olarak değerlendirileceğine, bu durumda olan yurt dışında yerleşik tüzel kişilerin Türkiye'deki şubeleri için Kişisel Verileri Koruma Kurulunun 2018/88 sayılı ve 2019/265 sayılı kararlarında yer alan "yıllık çalışan sayısı" ve "yıllık mali bilanço toplamı" kriterleri açısından yapılacak değerlendirme sonucunda Sicile kayıt yükümlülüğü bulunup bulunmadığına karar verileceğine, bu durumda olmayan yurt dışında yerleşik tüzel kişilerin Türkiye'deki şubelerinin ise Sicile kayıt yükümlülüğünün bulunmadığına,

c) Türkiye'de irtibat bürosu açılabilmesi için şirket tüzel kişiliklerinin yabancı ülke kanunlarına göre kurulması ve kurulan irtibat bürolarının Türkiye'de ticari faaliyette bulunmaması gerektiği, irtibat bürolarının ticari faaliyet dışında haberleşme, fizibilite araştırması yapma, sosyal ve kültürel

Decision Summary

The Personal Data Protection Board's decision upon request of their opinion;

"a) Directly or through branches in Turkey and abroad in the personal data processing activities of the resident company responsible for the data registers must be registered

b) Branches of legal entities residing abroad of branches in Turkey, setting by definition responsible for the data contained in the law of personal data processing objectives and means and the establishment of a data recording system if responsible for managing the separate legal entity located abroad resident data as responsible in Turkey will be evaluated. In this case, in terms of legal entities, the Personal Data Protection Board 2018/88 dated and 2019/265 dated Situated in the decision for branches in Turkey, "the annual number of employees" and "annual financial balance sheet total" criteria for the evaluation to be made in terms of presence Registry registration obligation that will be decided. Branches that are not in this situation have no obligation to register in the Registry.

c) For open liaison offices in Turkey for companies residing abroad, they should be established according to the laws of the foreign legal entity. These offices cannot make any commercial activities. These are the offices that are opened for the purpose of communication, feasibility research, conducting some studies in social and cultural areas, making preparations for mergers and transfers between companies, promotion and advertising, closely

alanlarda bazı çalışmaları yürütme, şirketler arasında birleşme ve devirler için ön hazırlık yapma, tanıtım ve reklam, ülkedeki iş olanaklarının yakından takip etme ve bu konular hakkında merkez firmaya bilgi verme amacı doğrultusunda açılan bürolar olması ve şube özelliği bulunmadığı hususu dikkate alındığında söz konusu irtibat bürolarının Sicile kayıt olma yükümlülüğünün bulunmadığına"

karar verilerek yurtdışında yerleşik olan ancak şube veya irtibat büroları aracılığıyla ülkemizde faaliyet gösteren tüzel kişilere ve onların şube veya irtibat bürolarına ilişkin veri sorumluluğu kapsamında sicile kayıt yükümlülüğü mercek altına alınmıştır.

Karar Işığında Veri Sorumlusu Kavramı

❑ 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 16. maddesinde, kişisel veri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorunluluğunun bulunduğuna ilişkin düzenleme yapılmış ve bu zorunluluğa ancak işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle ve yalnızca Kurul tarafından istisna getirilebileceği belirtilmiştir.

❑ Kurul tarafından verilen söz konusu kararı değerlendirmek açısından öncelikle "veri sorumlusu" kavramının mevzuat kapsamında değerlendirilmesi faydalı olacaktır. 7 Nisan 2016 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nun tanımlar kısmında veri sorumlusu "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak açıklanmıştır. Buna göre bir veri sorumlusundan söz edilebilmesi için öncelikle gerçek ya da tüzel kişiliğe haiz olunması gerekmektedir. Bunun yanı sıra veri sorumlusu gerçek ya da tüzel kişi; kişisel veri işleme süreci boyunca işlenen bu verilerin ne amaçla ve hangi yolla işleneceği, ilgili kişilerden elde edilen verilerin nasıl bir kayıt sistemine entegre edilip veri işleme sürecinin ne şekilde kontrol edileceği, işlenen verilerin ne kadar süre saklanacağı gibi önemli hususlarda karar merci olarak tasarrufta bulunabilmek durumundadır.

Sonuç

Kişisel Verilerin Korunması Kurulu tarafından verilen karar kimlerin veri sorumlusu olarak nitelendirileceğini ve bu bağlamda kimlerin VERBİS'e kayıt yükümlülüğünün bulunduğunu ortaya koymuştur. Gerek yurtdışı kaynaklı yatırımlar, gerek ise dünyada hizmet sektörünün ülkesel sınırları aşması sebebiyle yerli tüzel kişiler olduğu gibi yurtdışında yerleşik bulunan yabancı tüzel kişiler de şube açarak ya da irtibat bürosu kurarak ülkemizde faaliyet

following the job opportunities in the country and informing the central firm about these issues. These liaison offices don't have an obligation to register in the Registry, because of they don't have any characteristics about branches."

The Concept of Data Controllers in the Light of Decision

❑ In Article 16 of the Law on the Protection of Personal Data No.6698, a regulation has been made that natural and legal persons who process personal data are obliged to register with the Data Controllers Registry before starting data processing. It has been stated that an exception can only be made by the Board, taking into account objective criteria to be determined by the Board, such as the nature and number of personal data processed under this obligation, the data processing originating from the law or the status of their transfer to third parties.

❑ In order to evaluate the decision made by the Board, it would be useful to first consider the concept of "data controller" within the scope of the legislation. In the definitions section of the Personal Data Protection Law, which entered into force on April 7, 2016, the data controller is explained as "the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system". Accordingly, in order to mention a data controller, it is necessary to have a natural or legal personality first. In addition, the natural or legal person responsible for the data; It has to be able to make savings as a decision-maker in important matters such as for what purpose and in what way these data processed during the personal data processing process will be processed, how the data obtained from the relevant persons will be integrated into a recording system and how the data processing process will be controlled, and how long the processed data will be stored.

Conclusion

❑ The decision made by the Personal Data Protection Board explained who will be considered as the data controller and in this context, who has the obligation to register in the data registry. Due to the investments originating from abroad and because the service sector in

göstermektedir. Bu faaliyetler beraberinde birtakım kişisel veri işleme işlemini de beraberinde getirmekte, veri işleyen şube ya da irtibat bürosu açısından veri sorumlusu olup olmadıkları akla gelmektedir. Bu konuda tereddüte yer bırakmayacak şekilde Kurul tarafından verilen kararda; yerleşim yeri yurt dışında bulunan tüzel kişilerin Türkiye'deki şubelerinin, kendi bünyesindeki kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemesi ve veri kayıt sistemlerinin kurulması ile yönetilmesinden sorumlu olmaları halinde tüzel kişiden bağımsız bir veri sorumlusu sıfatına haiz olacakları belirtilmiştir. Söz konusu şubelerin veri sorumlusu sayılmalarının en önemli sonucu olarak VERBİS'e kayıt yükümlülüklerinin bulunup bulunmadığı *"yıllık çalışan sayısı" ve "yıllık mali bilanço toplamı"* kriterleri açısından yapılacak değerlendirme sonucunda karara bağlanacaktır. Türkiye'de kurulan irtibat büroları ise, tanıtım ve reklam, ülkedeki iş olanaklarının yakından takip etme ve bu konular hakkında merkez firmaya bilgi verme amacı doğrultusunda açılan bürolar olduklarından ve şube özelliği taşımadıklarından VERBİS'e kayıt yükümlülükleri bulunmamaktadır.

the world crosses the national borders, foreign legal entities residing abroad operate in our country by opening branches or establishing liaison offices. These activities bring along some personal data processing operations, and it comes to mind whether they are data controllers for the data processing branch or liaison office. No question marks were left in minds with the clear decision of the Board on this matter. Branches in Turkey of legal entities which located abroad, will be conferred to an independent data controller for the capacity of legal persons if they are responsible for managing with the aim of processing of personal data in their own systems and the establishment of determining the tools and data recording system. As the most important result of the said branches being accepted as data controller, it will be decided as a result of the evaluation to be made in terms of "annual number of employees" and "annual financial balance sheet total" criteria. On the other hand, liaision offices only make activities about promotion, advertising and don't have an obligation to register in the Registry, because of they don't have any characteristics about branches.

Kişisel Verilerin Korunması Kanunu Çerçevesinde Türkiye'den Yurt Dışına Kişisel Veri Aktarımı

Av.Ayşe Hüma Lofça

Genel Bilgi

❑ Günümüzde doğrudan yabancı yatırım Türkiye de dahil olmak üzere her ülkenin ekonomisinde zorunlu bir unsur haline gelmiştir. Ülkeler yurtdışında yatırım yaparken, kişisel verileri işler. Veri korumanın önemi arttıkça, yabancı yatırımcılar uluslararası aktarılan veriler ve uygulanacak kurallar ile ilgili sorularla baş başa kalır. Bu makalede, Türkiye'den yurt dışına aktarılabilecek kişisel verilerin kapsamı ve 24/3/2016 tarihli ve 6698 sayılı "Kişisel Verilerin Korunması Kanunu" irdelenecektir.

❑ Türkiye'de yapılan yabancı yatırımlar, Türkiye'de uygulanan kişisel veri koruma hükümleri göz önünde bulundurularak yapılmalıdır. Yatırımcıların kendi ülkelerinden işçi getirmeleri, Türk veya yabancı işçi istihdam etmeleri fark etmeksizin çeşitli kişisel veri türleri Türkiye'de işlenecek ve böylece Türk veri tabanının bir parçası haline gelecektir. Bu durumda, doğrudan yabancı yatırımcılar verinin işlenmesi ve aktarımı sırasında Türk hukukunu göz önünde bulundurmalıdırlar.

Kişisel Verilerin Korunması Kanunu

❑ Kişisel Verilerin Korunması Kanunu'nun 9. Maddesi, yurt dışına veri aktarımı kuralını ortaya koymaktadır. Söz konusu maddenin birinci fıkrasına göre kişisel veriler yurt dışına ilgili kişinin açık rızası olmaksızın aktarılamaz. Yurtdışına yapılacak tüm veri transferleri, ilgili kişinin bilgisi ve rızası dahilinde olmalıdır.

❑ İkinci paragraf, kuralın istisnalarını belirtir; kişisel verilerin yurt dışına ilgilinin açık rızası olmaksızın aktarılabilmesi için verilerin aktarılacağı yabancı ülkede yeterli koruma bulunması veya yeterli koruma bulunmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulun izninin bulunması gerekmektedir.

❑ Ayrıca, yabancı ülkede yeterli koruma bulunup bulunmamasına bakılmaksızın, madde 5/2 veya madde 6/3'te belirtilen şartlardan birinin yerine getirilmesi gerekir. İlk olarak yeterli korumaya sahip yabancı ülkelerin durumu incelenecektir.

Foreign Direct Investment and Personal Data Transfer Abroad Within The Framework of The Law on The Protection of Personal Data in Turkey

General Information

❑ In today's world, foreign direct investment has become a crucial component in almost every country's economy, including Turkey. While countries invest abroad, they process personal information and as the importance of data protection increases, foreign investors are left with questions about internationally transferred data and the rules to be applied. This article will discuss the scope of personal data in Turkey which can be transferred abroad and the binding law such as the Turkish "Law on The Protection of Personal Data" dated 24/3/2016, No: 6698.

❑ Foreign direct investments made in Turkey must be in compliance with the data protection laws applied in Turkey. Whether investors choose to employ Turkish workers, bring in workers from their home country or from foreign countries, various kinds of personal data will be processed in Turkey, making the personal data of these workers a part of the Turkish data base. In this sense, foreign direct investors must take into consideration that processing and transferring of such data must be done according to the Turkish law on data protection.

The Law on Personal Data Protection

❑ Article 9 of the "Law on the Protection of Personal Data" lays out the rule for data transfer abroad. According to the first paragraph of said article, the transfer of personal data abroad is prohibited without explicit consent of the data subject. All data transfers abroad must be within the knowledge and consent of the data subject.

❑ The second paragraph states exceptions to the rule; personal data can be transferred abroad without explicit consent if the foreign country where the data is to be transferred provides sufficient protection or if sufficient protection is not provided, the Personal Data Protection Board must authorize the transfer based on an agreement between the controllers in Turkey and in the related foreign country.

❑ Furthermore, one of the conditions set forth in either Article 5-Paragraph 2 or Article 6-Paragraph 3 must be met whether the foreign country provides sufficient protection or not. The case of foreign countries with sufficient protection will be examined first.

Türkiye'den Yeterli Korumaya Sahip Ülkelere Kişisel Veri Aktarımı

❑ Kişisel Verileri Koruma Kurumu yeterli koruma bulunan ülkeleri saptar ve ilan eder. Verinin aktarıldığı yabancı ülke yeterli korumaya sahip ülkeler arasında sayılıyorsa madde 5/2 veya madde 6/3 koşullarından biri sağlandığı takdirde veri aktarımı yapılabilir. Bu iki madde özel nitelikli kişisel veri olup olmamasına göre ayrılmaktadır.

Yeterli Korumaya Sahip Ülkelere Özel Nitelikli Kişisel Veri Aktarımı

❑ Madde 6/1'e göre özel nitelikli kişisel veriler, "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"dir. Özel nitelikli kişisel veriler ilgilinin açık rızası olmadan işlenemez.

❑ 6'ncı maddenin 3'üncü fıkrası kuralın istisnalarını öngörür. Bu durumda, cinsel hayat veya sağlığa ilişkin olan veriler dışındaki özel nitelikli kişisel veriler kanunda öngörüldüğü takdirde ilgili kişinin açık rızası alınmadan işlenebilir.

❑ Sağlık veya cinsel hayata ilişkin kişisel veriler ancak;

- Kamu sağlığının korunması amacıyla,
- Koruyucu hekimlik için,
- Tıbbî teşhis için,
- Tedavi ve bakım hizmetlerinin yürütülmesi için,
- Sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla,

sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

❑ Veri işlenmesi faydalı veri tabanları oluşturulması ve kamu ihtiyaçlarının daha iyi yönetilmesi için zorunlu bir unsurdur ancak işlenen verinin niteliği özelleştikçe kanun maddeleri daha katı hale gelir. Yukarıda görüldüğü üzere sağlık ve cinsel hayat gibi çok özel kişisel veriler ancak önemli hususlar için ilgilinin rızası olmadan işlenebilmektedir.

Özel Nitelikli Olmayan Kişisel Verilerin Yeterli Korumaya Sahip Ülkelere Aktarımı

❑ Özel nitelikli olmayan kişisel veriler için daha geniş bir kapsam öngörülmüştür. 5'inci maddenin 2'nci fıkrası uyarınca bu tür kişisel veriler yurtdışına ilgilinin rızası olmadan aşağıdaki hallerde aktarılabilir;

"a) Kanunlarda açıkça öngörülmesi.

Data Transfers from Turkey to Countries with Sufficient Protection

❑ The Personal Data Protection Board shall announce the countries deemed sufficiently protected. If the foreign country receiving the data transfer is listed as a sufficiently protected country, either Article 5/2 or Article 6/3 must be met for the transfer to be made. These two articles differentiate on terms of whether the data is of special nature.

Transferring Special Categories of Personal Data to Countries with Sufficient Protection

❑ Special categories of personal data entails "race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data" as stated in Article 6/1. Special categories of personel data cannot be processed without explicit consent from the data subject.

❑ The third paragraph of this article lays down the exception to the rule. Personal data, other than those related to sexual life or health may be processed without explicit consent if it is prescribed by laws.

❑ Personal data related to health or sexual life can be processed without explicit consent only for;

- Public health protection purposes,
- Operation of preventative medicine,
- Medical diagnosis,
- Treatment and nursing services,
- The planning and management of health-care services and their financing,

by persons or authorized institutions and organizations under a confidentiality obligation.

❑ Data processing is a necessary element for creating efficient databases to better serve public needs but strict regulations are needed as the data gets more personal. As seen above, very personal data subjects such as sexual life and health may only be processed without consent for matters of greater importance.

The Transferring of Data Other Than Special Categories of Personal Data to Countries with Sufficient Protection

❑ Other than those of special categories of personal data has a wider scope of applicability as opposed to those of special nature. According to Paragraph 2 of Article 5, this type of data can be transferred abroad without explicit consent if;

"a) It is clearly provided for by the laws.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

Türkiye'den Yeterli Korumaya Sahip Olmayan Ülkelere Veri Aktarımı

❑ Verinin aktarılacağı ülkede yeterli koruma bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri gerekmektedir ve ayrıca Kurulun izni gerekmektedir. Madde 9/4'te Kurulun vereceği izin aşağıdaki koşullara bağlıdır;

"…a)Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,
değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.
(5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.
(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

❑ Ayrıca madde 5/2 veya 6/3'teki şartlardan biri sağlanmalıdır. Ancak o halde veri aktarımı ilgilinin açık rızası olmadan yurtdışına aktarılabilir.

❑ Türkiye'den yeterli koruma bulunmayan ülkelere veri aktarımı yapılırken madde 9/2 uyarınca yazılı taahhüt

b) it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.
c) processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfillment of that contract.
ç) it is mandatory for the controller to be able to perform his legal obligations.
d) the data concerned is made available to the public by the data subject himself.
e) data processing is mandatory for the establishment, exercise or protection of any right.
f) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject."

Data Transfers from Turkey to Countries without Sufficient Protection

❑ If the country in which the personal data will be transferred does not provide sufficient protection, both the controllers in Turkey and in the foreign country must guarantee sufficient protection in writing and is subject to the Board's authorization. According to Article 9/4, the Board will authorize the written agreement on the grounds of;

"…a) The international conventions to which turkey is a party,
B) The state of reciprocity relating to data transfer between the requesting country and Turkey,
C) The nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer,
Ç) The relevant legislation and its implementation in the country to which the personal data are to be transferred,
D) The measures committed by the data controller in the country to which the personal data are to be transferred,
5) Without prejudice to the provisions of international agreements, in cases where interest of Turkey or the data subject will seriously get harmed, personal data, may only be transferred abroad upon the authorization to be given by the board after receiving the opinions of relevant public institutions and organizations.
6) the provisions of other laws relating to the transfer of personal data abroad are reserved."

❑ In addition, one of the conditions set forth in articles 5/2 or 6/3 must apply. Only then is data transferring without explicit consent accepted.

❑ While transferring data from Turkey to countries without sufficient protection, according to Article 9/2, a written guarantee is mandatory and the following matters

verilmelidir. Aşağıdaki hususlar asgari olarak taahhütte bulunmalıdır.

Veri Aktaranın Taahhütnameden Kaynaklanan Yükümlülükleri

❑ Kişisel veriler, Kişisel Verileri Koruma Kanunu'na uygun olarak işlenmelidir. Burada veriyi aktaran veri sorumlusu, hem kendi yükümlülüklerini yerine getirmek hem de veri alıcısının yükümlülüklerini yerine getirmesini denetlemek zorundadır.

❑ Veri aktaran, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak için kişisel verinin niteliğine göre uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almalıdır. Ayrıca veri alıcısının da bu tedbirlerin alındığından emin olmalıdır.

❑ Veri aktaran, veri alıcısını KVKK ve ilgili diğer mevzuat hakkında bilgilendirir. Veri aktaran, kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede kendisine bildirmek zorunda olduğunu veri alıcısına bildirir. Veri aktaran, bu durumu ilgilisine ve Kişisel Verileri Koruma Kuruluna en kısa sürede bildirir. Kurul, gerekli görürse bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

❑ Veri aktaran, veri alıcısının sözleşme hükümlerini yerine getirmesiyle ilgili meydana gelebilecek sorunları derhal Kurul'a bildirmekle yükümlüdür. Veri alıcısının ilgili kişilerden ve Kurul'dan gelen soruları cevaplaması kararlaştırılmış olmasına rağmen cevap vermesi mümkün olmadığı durumlarda veri aktaran, elindeki tüm bilgi ve belgelerle makul bir süre içerisinde ilgili kişi veya Kurul'un sorularını cevaplandırır.

❑ Veri aktaran, veri alıcısı sözleşmeye ilişkin sorumluluklarını yerine getirmediği takdirde sözleşmeyi askıya alma veya feshetme hakkına sahiptir. Askıya alma veya feshedilme derhal Kurul'a bildirilir.

Veri Alıcısının Taahhütnameden Kaynaklanan Yükümlülükleri

❑ Veri alıcısı, hukuka aykırı olarak veri işlenmesi, erişilmesi ve kişisel verilerin muhafazası için uygun güvenlik düzeyinin temini için gerekli her türlü teknik ve idari tedbiri almakla yükümlüdür.

❑ Kişisel verilerin veri alıcısı adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde gerekli tedbirlerin alınması konusunda bu kişilerle birlikte müştereken sorumludur. Veri işleyenler de dahil olmak üzere veri alıcısının yetkisi altında çalışan kimseler ancak verilen

must take place in said guarantee.

Obligations of the Controller Transferring Data Regarding the Guarantee Agreement

❑ Personal data must be processed and transferred in accordance with the Law on the Protection of Personal Data. The controller who is transferring the data undertakes great responsibility throughout the process because while fulfilling their own obligations they must also supervise the receiving controller's actions.

❑ The transferring controller must take measures to insure the prevention of unlawful processing, unlawful accessing and must provide sufficient security for any technical or administrative measures and must also make sure that the receiving controller takes said measures.

❑ The transferring controller will notify the receiving controller about the LPPD and other regulations about data protection. The transferring controller must notify the receiving controller that in case of personal data being obtained by third parties unlawfully, the receiving controller shall report such incident to the transferring controller immediately. The transferring controller will then notify the Board and the subject of data. The Board may announce the incident on its website or another method deemed appropriate.

❑ The transferring controller is obligated to notify the Board of any problems that may arise surrounding the guarantee. If the receiving controller is unable to answer queries directed by related persons or the Board despite it being agreed upon, the transferring controller is obligated to provide answers in the light of the information available to them.

❑ The transferring controller may suspend data transferring or terminate the contract if the receiving data controller violates the obligations. Suspensions or terminations are immediately notified to the Board.

Obligations of the Controller Receiving Data Regarding the Guarantee Agreement

❑ The receiving controller must take measures to insure the prevention of unlawful processing, unlawful accessing and must provide sufficient security for any technical or administrative measures.

❑ In case of personal data being processed on the controller's behalf by another natural or legal person, these persons and the controller will be jointly liable. Data processors included, persons operating under the authority of the controller may only process data in accordance with their given instructions. If for any reason, compliance with the laws and the agreement is not

talimatlara uygun olarak veri işlemeye yetkilidir. Herhangi bir sebeple sözleşme hükümleri uygulanamazsa derhal veri aktarana bildirilmelidir.

❑ Veri aktaran, veri alıcısı sorumluluklarını yerine getirmediği takdirde askıya alma veya feshetme hakkına sahiptir. Veri alıcısı, sözleşmeye aykırı ulusal düzenleme olmadığını kabul, beyan ve taahhüt eder. Ayrıca veri aktaran, veri alıcısının yükümlülüklerini yerine getirmesi konusunda denetim yapma hakkına sahiptir.

❑ Sözleşmedeki taahhütlerin yerine getirilmesini etkileyecek bir mevzuat değişikliği yapılması halinde veya adli makamlardan bir talep geldiği takdirde veri alıcısı hemen durumu veri aktarana bildirmek zorundadır.

❑ Sözleşmenin feshedilmesi veya askıya alınması durumunda veri aktaranın tercihine göre, aktarılmış olan kişisel veriler için iki durum söz konusudur. Yedekleri de dahil olmak üzere aktarılan tüm kişisel veriler, veri aktarana geri gönderilebilir veya veri alıcısı verileri tamamen yok eder. Mevzuatta kişisel verilerin yok edilmesini engelleyen hükümler varsa aktarılan kişisel verilerin gizliliğini güvence altına almak için gerekli tüm idari ve teknik tedbirleri alır ve veri işleme faaliyetini durdurur.

❑ Sözleşmeye istinaden veri aktarımı gerçekleştirilirken, veri alıcısının kişisel verileri bir alt işverene aktarması gerekirse veri alıcısının veri aktaranı ispat edilebilir bir şekilde bilgilendirme ve onayını alma sorumluluğu vardır. Veri alıcısı ve alt işveren arasında yapılan sözleşme asgari olarak veri aktaran ve veri alıcısı arasındaki sözleşme hükümlerini içermelidir.

Taahhütnamenin Ortak Hükümleri

❑ Her iki tarafın kişisel verileri KVKK hükümlerine aykırı olarak üçüncü kişilere aktaramaz. Kişisel verileri yalnızca işleme amacıyla kullanabilir. Bu yükümlülük veri aktaran ve alıcı açısından herhangi bir süre sınırı yoktur.

achieved, it must be notified to the transferring controller immediately.

❑ The transferring controller holds the right to suspend or terminate the agreement if the receiving controller fails to fulfill any obligations related to the guarantee agreement. The receiving controller must accept and guarantee that there are no contradicting national regulations to the agreement. Furthermore, the transferring controller is authorized to supervise the actions of the receiving controller.

❑ If any legislation changes may affect the compliance to the agreement or if any request from a judicial authority is directed to the receiving controller, the transferring controller must be notified immediately.

❑ In case of the termination of the agreement or if the validity period is over, depending on the choice of the controller transferring data, the personal data being transferred including their backups will either be sent back to the controller transferring the data or the personal data will be terminated completely. If there are any statutes preventing the receiving data controller from executing this obligation, the receiving controller must accept to take any technological and administrative measures to insure confidentiality and stop the data processing activity.

❑ While performing the service regarding the agreement, if it is necessary for the receiving controller to transfer personal data to a subcontractor, the transferring controller must be notified in an evincive manner. Approval of the transferring controller is mandatory. The agreement between the subcontractor and the receiving controller must at a minimum, include the provisions of the agreement between the transferring controller and receiving controller.

Common Provisions Regarding the Guarantee Agreement

❑ Both parties cannot disclose the personal data being processed to anyone outside of the LPPD provisions and cannot use the data for purposes other than processing. This obligation is not limited to any period of time for the two parties.

Sosyal Ağ Sağlayıcılarının Yükümlülükleri ve Bu Yükümlülüklere Aykırı Davranılması Halinde Uygulanacak Yaptırımlar

Av.Meryem Kılıç
Av.Ayşe Hüma Lofça

❑ Bilgi Teknolojileri İletişim Kurumu 29.09.2020 tarihinde verdiği karar ile sosyal ağ sağlayıcılarının yükümlülüklerini belirledi. Anılan karar 02.10.2020 tarihinde yürürlüğe girdiğinden, bu karar kapsamında yükümlülüklerin neler olduğu ve bu yükümlülüklere aykırı davranılması halinde uygulanacak yaptırımlar sosyal ağ sağlayıcıları açısından önem arz etmektedir.

❑ Söz konusu karar Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcılarını kapsamaktadır. Bu kararın uygulanmasında, internet ortamında yapılan yayının sadece belirli bir kısmında sosyal etkileşim amaçlı içeriğe yer veren gerçek veya tüzel kişiler sosyal ağ sağlayıcı olarak değerlendirilmeyecektir. Yine kişisel internet siteleri, elektronik ticaret siteleri ve haber siteleri gibi sosyal etkileşim amaçlı içeriğin ikincil ve yan bir hizmet olarak sunulduğu platformlar da kararda belirtilen yükümlülüklerin kapsamı dışındadır. Karar kapsamında belirlenen yükümlülükler şunlardır;

Temsilci Belirleme Yükümlülüğü Nedir?

❑ Yukarıda verilen kapsamda yer alan yurtdışı ağ sağlayıcıları, yetkili en az bir kişiyi Türkiye'de temsilci olarak belirlemekle yükümlüdür. Temsilci veya temsilciler, gerçek veya tüzel kişi olabilir. Gerçek kişilerin Türkiye'de ikamet etmesi gerekmektedir. Tüzel kişi olarak belirlenen temsilci veya temsilcilerin, Türkiye'de kurulmuş ve Türk mevzuatına göre tüzel kişiliğini kazanmış olması; gerçek kişi olarak belirlenen temsilci veya temsilcilerin ise Türk vatandaşı olması zorunludur.

❑ Sosyal ağ sağlayıcıları, temsilci veya temsilcilerin kimlik, unvan ve iletişim bilgilerini Bilgi Teknolojileri ve İletişim Kurumuna bildirmekle yükümlüdür.Bildirilen bilgilerde değişiklik olması durumunda, bu değişiklikler derhal ve en geç yirmi dört saat içinde Kuruma bildirilir.

❑ Sosyal ağ sağlayıcıları, tarafından kuruma bildirilen temsilci veya temsilcilerin Türkiye'deki tebligata yarar adresi ile e-posta adresine, kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer vermek zorundadır. Eğer belirlediği temsilcisinin kayıtlı elektronik posta adresi varsa yine bu bilgiyi de internet sitesine eklemekle yükümlüdür.

❑ Ayrıca temsilci veya temsilcilerin iletişim bilgilerinde sonradan değişiklik olması durumunda, bu değişikliklere derhal internet sitesinde yer verilmelidir.

The Obligations of Social Network Providers and Sanctions to Be Applied in Case of Breach

❑ The Information Technologies and Communication Institution determined the obligations of social network providers with it's 29.09.2020 dated decision. Said decision went into force on 02.10.2020, making the obligations of this decision and the sanctions of breach of great importance.

❑ This decision covers social network providers with more than one million daily access rates both nationally and internationally. In the implementation of this decision, natural or legal social network providers with specific social interaction based content won't be accepted as social network providers. Personal websites, e-commerce sites and news sites where social interaction based content is a side service will be outside the scope of these obligations. The obligations within the scope are shown below;

What is The Obligation to Appoint a Representative?

❑ Foreign network providers are obligated to determine at least one representative in Turkey. Representatives may be natural or legal persons. Natural persons must be residing in Turkey. Legal persons appointed as a representative must have been founded in Turkey and gained legal personality in compliance with Turkish law.

❑ Social network providers are obligated to notify the Information Technologies and Communication Institution of the representative's identification, title and contact information. If any change occurs, they must be reported to the Institution immediately, within twenty-four hours at the latest.

❑ The social network providers must provide the address which can be notified in Turkey and e-mail of the representatives on their website in an easily visible and directly accessible manner. The changes of contact information of the representatives must be published on said website.

Temsilci Belirleme Yükümlülüğüne Uyulmaması Halinde Karşılaşılacak Yaptırımlar Nelerdir?

İdari Para Cezası Uygulanması

❑ Temsilci belirlenmesine ilişkin yükümlülüklerini yerine getirmeyen sosyal ağ sağlayıcıya, Bilgi Teknolojileri ve İletişim Kurumu tarafından bildirimde bulunulur. Bildirimden itibaren otuz gün içinde temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmemesi hâlinde, sosyal ağ sağlayıcıya Başkan tarafından onmilyon Türk Lirası idari para cezası verilir. Verilen idari para cezasının tebliğinden itibaren otuz gün içinde temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmemesi hâlinde, Başkan tarafından bir kez daha otuz milyon Türk lirası idari para cezası verilir.

❑ Temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmesi hâlinde; verilen idari para cezalarının dörtte biri tahsil edilir.

Reklam Yasağı Uygulanması

❑ İkinci kez verilen idari para cezasının tebliğinden itibaren otuz gün içinde temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmemesi hâlinde, Başkan tarafından Türkiye'de mukim vergi mükellefi olan gerçek ve tüzel kişilerin ilgili sosyal ağ sağlayıcısına yeni reklam vermesi yasaklanır. Reklam yasağı kararı uyarınca, sosyal ağ sağlayıcıyla yeni sözleşme kurulamaz ve sosyal ağ sağlayıcıya para transferi yapılamaz. Başkan tarafından verilen reklam yasağı kararı yayımlanmak üzere Resmî Gazete'ye gönderilir. Resmî Gazete'de yayımlanan reklam yasağı kararının uygulanmasına ilişkin hususlar, ilgili kamu kurum ve kuruluşları tarafından takip edilir.

❑ Temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmesi hâlinde; reklam yasağı kaldırılır.

İnternet trafiği bant genişliğinin daraltılması

❑ Reklam yasağı kararının verildiği tarihten itibaren üç ay içinde temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmemesi hâlinde Başkan, sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde elli oranında daraltılması için sulh ceza hâkimliğine başvurabilir.

❑ Başvurunun kabulüne ilişkin hâkim kararının uygulanmasından itibaren otuz gün içinde temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmemesi hâlinde Başkan, sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde doksan oranına kadar daraltılması için sulh ceza hâkimliğine başvurabilir. Hâkim internet trafiği bant genişliğinin yüzde doksan oranına kadar daraltılması hakkında vereceği kararında

What sanctions will be applied if the obligation to appoint a representative is breached?

Administrative Fines

❑ The Information Technologies and Communications Institution will notify the social network provider who failed to comply with the obligations. If the obligations to determine a representative are not met within thirty days of the notification, the President with issue a ten million Turkish Lira administrative fine. If the obligations are not met for another thirty days, the network provider will be fined thirty million Turkish Liras.

❑ If the obligations are met, one fourth of the fine will be collected.

Advertisement Bans

❑ If the obligations are not fulfilled within thirty days of the second fine notification, natural or legal resident taxpayers in Turkey will be prohibited from advertising on their website. According to the advertisement ban, a new agreement cannot be made with this network provider, nor can Money be transferred to this network provider. The advertisement ban will be sent to the Official Newspaper. The Official Newspaper will then publish the ban and will be followed by related public institutions and organizations.

❑ When obligations regarding representative determination are met, the advertisement ban will be lifted.

Constriction of the Internet Traffic Bandwidth

❑ Within three months of the advertisement ban decision, if obligations are still unfulfilled, the President will apply to the Criminal Court of Peace for the bandwidth of internet traffic to be constricted by fifty percent.

❑ In case of failure to fulfill the obligations regarding the appointment of a representative within thirty days after the decision of the Court regarding the acceptance of the application, the President may apply to the Criminal Court of Peace to reduce the internet traffic bandwidth of the social network provider up to ninety percent. In his decision about reducing the internet traffic bandwidth up to ninety percent, the Court may determine a rate on the

yüzde elliden düşük olmamak kaydıyla, sunulan hizmetin niteliğini de dikkate alarak bir oran belirleyebilir. Hâkim tarafından verilen kararlara karşı Başkan tarafından 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

❑ Temsilci belirlenmesine ilişkin yükümlülüklerin yerine getirilmesi hâlinde; hâkim kararları kendiliğinden hükümsüz kalır. İnternet trafiği bant genişliğine yapılan müdahalenin sona erdirilmesi için erişim sağlayıcılara Kurum tarafından bildirim yapılır.

Kişiler Tarafından Yapılan Başvuruların Cevaplandırılması Yükümlülüğü Nedir ?

❑ Yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, 5651 sayılı *"Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla işlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*un 9 ve 9/A maddeleri kapsamındaki içeriklere yönelik olarak kişiler tarafından yapılacak başvurulara cevap vermekle yükümlüdür.

❑ Sosyal ağ sağlayıcı, kişiler tarafından yapılacak bu başvuruların kolaylıkla alınabilmesi ile başvurunun Türkçe dil seçeneği kullanılarak yapılabilmesini sağlar.

❑ Sosyal ağ sağlayıcı, başvurulara başvurudan itibaren en geç kırk sekiz saat içinde olumlu ya da gerekçesi belirtilmek kaydıyla olumsuz cevap verir. Türkçe yapılan başvuruların Türkçe cevaplanması zorunludur.

Kişiler Tarafından Yapılan Başvuruların Cevaplandırılması Yükümlülüğünün Yerine Getirilmemesi Halinde Karşılaşılacak Yaptırımlar Nelerdir?

❑ Kişiler tarafından yapılan başvuruların cevaplandırılması yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcıya Bilgi Teknolojileri ve İletişim Kurumu Başkanı tarafından beş milyon Türk Lirası idari para cezası verilir.

❑ Kurum, başvurucunun şikâyeti üzerine, sosyal ağ sağlayıcının yükümlülüğün yerine getirilip getirilmediğini inceler. Kurum, birinci fıkrada belirtilen yükümlülüğün yerine getirilmediği gerekçesiyle yapılan başvuruları raporlama dönemlerinde toplu olarak değerlendirir.

❑ Kurum tarafından yapılacak değerlendirmede; sosyal ağ sağlayıcının yükümlülüğünü etkin bir şekilde yerine getirmek için gerekli sistemleri kurup kurmaması, Sosyal ağ sağlayıcının belirli kişilere veya kurumlara düzenli olarak olumsuz cevap vermesi, Başvurulara verilen olumsuz cevapların gerekçesiz olması, hususları göz önünde bulundurulur.

basis of the nature of the service given, provided that it is not less than fifty percent, The President may appeal against the decisions made by the Court in accordance with the provisions of the Criminal Procedure Law No. 5271, dated 4/12/2004.

❑ In case of the obligations to appoint a representative are fulfilled; Court decisions are automatically voided. The Authority makes a notification to the access providers in order to terminate the intervention to the internet traffic bandwidth.

What İs the obligation to answer applications?

❑ The social network provider of domestic or foreign origin is obliged to respond to the applications made by individuals for the contents within the scope of articles 9 and 9 /A of the Law No. 5651 on "Regulation of Broadcasts Made on the Internet and Fighting Against Crimes Committed Through These Publications".

❑ The social network provider must ensure that these applications can be easily received by individuals and the application can be made using the Turkish language option.

❑ The social network provider must respond positively or negatively, provided that the reason is stated, within 48 hours at the latest from the application. Applications made in Turkish must be answered in Turkish.

❑ What Sanctions Will Be Applied if The Obligatıon To Answer Applications Are Unfulfilled?

❑ Social network providers who do not comply with the obligation to answer applications will be fined five million Turkish Liras by the President.

❑ The Institution will examine whether or not the social network provider has met it's obligations upon the complaint of the applicant. The institution will examine applications regarding unfulfilled obligations as a whole during reporting periods.

❑ In the Institution's examination, factors such as whether necessary systems for the fulfillment of the obligations are built by the social network providers, whether the social network providers are consistently giving a negative response to applications, whether these negative responses are unjustified will be taken into account.

Raporlama Yükümlülüğü Nedir?

❑ Yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, kendisine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve kişiler tarafından yapılacak başvurulara ilişkin, istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları altı aylık dönemlerle Bilgi Teknolojileri ve İletişim Kurumu'na bildirmekle yükümlüdür.

❑ Ayrıca kişilerin başvurularına ilişkin sosyal ağ sağlayıcı tarafından hazırlanan rapor, kişisel verilerden arındırılmak suretiyle sosyal ağ sağlayıcının kendi internet sitesinde de yayınlanmalıdır.

Raporlama Yükümlülüğünün Yerine Getirilmemesi Halinde Karşılaşılacak Yaptırımlar Nelerdir?

❑ Raporlama yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcıya Bilgi Teknolojileri ve İletişim Kurumu Başkanı tarafından on milyon Türk Lirası idari para cezası verilir.

Kurumun Verdiği İdari Para Cezalarına Karşı Yargısal Denetim

❑ Bilgi Teknolojileri ve İletişim Kurumu tarafından verilen idari para cezalarının yargısal denetimi; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda madde 8/12'de yer alan "Bu Kanunda tanımlanan kabahatler dolayısıyla Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir" şeklindeki özel hüküm nedeniyle, idari yargıda yapılması gerekmektedir. Bir idari organ olarak BTK tarafından verilen idari para cezalarına karşı İYUK Madde 32/1 uyarınca dava konusu olan idari işlemi veya idari sözleşmeyi yapan idari merciin bulunduğu yerdeki idare mahkemesi olarak Ankara idare mahkemelerinde iptal davaları açılabilecektir. İYUK madde 7'ye göre dava açma süresi kararın tebliğinden itibaren 60 gündür.

What is the Obligation of Reporting?

❑ Social network providers of domestic and foreign origin must present reports in Turkish of six month periods regarding the enforcement of removal and/or blocking of content decisions and statistics and categorized information regarding applications to the Information Technologies and Communication Institution.

❑ Furthermore, the report prepared by the social network provider must be cleansed from personal data and published on their own website.

What sanctions will be applied if the obligation of reporting is unfulfilled?

❑ Social network providers who fail to fulfill their reporting obligations will be fined ten million Turkish Liras by the President of the Information Technologies and Communication Institution.

Judicial Review of Administratıve Fines Given by The Institution

The Judicial review of administrative fines given by the Information Technologies and Communication Institution; Law No. 5651 on the Regulation of Broadcasts on the Internet and the Fight Against Crimes Committed Through these Publications Article 8/12 states that "Against administrative fines given by the Institution for misdemeanors defined in this law, legal remedies can be approached in accordance with the Law No. 2577 and dated 6/1/1982 on Administrative Trial Procedure." Due to this special provision, the review must be done in Administrative Jurisdiction. Against the fines given by the Information Technologies and Communication Institution, as an administrative body, according to Article 32/1 of the Administrative Trial Procedure Law, annulment actions can be pursued in Ankara Administrative Courts. These Ankara courts are the administrative courts located where the administrative authority issuing the administrative action and administrative agreements.

Kişisel Verilerin Korunması Hukuku Bülteni
Data Protection Law Bulletin

Bülten (Bulletin) No:1 **Ekim(October) 2020**

Torun Hukuk Bürosu;

Ankara'da konuşlu olan büromuz, sadece Ankara'da değil, tüm Türkiye'de, müvekkillerin hukuki problemlerinin çözülmesinde, yargılama ve idari makamlar nezdindeki dava ve hukuki işlemlerinin yürütülmesinde daima en kısa, en etkili ve sonuca giden en doğru yolu bulma hedefini düstur edinerek etik ilkelerden ödün vermeksizin başta Kişisel Verilerin Korunması Hukuku, İdari Yargı Hukuku, Arabuluculuk ve Hakemlik Hizmetleri, İnsan Hakları ve İnsancıl Haklar Hukuku, Ticaret Hukuku, İnşaat Hukuku, İş ve Sosyal Güvenlik Hukuku, Uluslararası Özel Hukuk, özlük haklarına ilişkin dava ve işlemler ile aşağıda belirtilen alanlarda tecrübeli avukat kadrosuna sahip bir hukuk bürosudur.

Amacımız, doğruluk ve dürüstlük ilkeleriyle bağlı bir şekilde, mevcut yargı sisteminde müdafi veya taraf sıfatıyla, hukukun bizlere sunduğu çerçeve içinde adaletin somut olarak ihtiyacı olan kişiye ulaşmasını sağlamaktır.

Mevcut avukat kadrolarımızla;

- Ceza Hukuku
- Borçlar Hukuku
- Aile Hukuku
- İcra ve İflas Hukuku
- Tüketici Hukuku
- Gayrimenkul ve Kat Mülkiyeti Hukuku alanlarında avukatlık hizmetleri sunmaktayız.

Torun Law Office;

At our firm while located in Ankara, have made it our vision to help our clients, not only in Ankara but in Turkey, by finding the shortest, most effective and correct way leading to solutions of legal issues, the execution of lawsuits and legal proceedings before the judicial and administrative authorities without compromising ethical values. At Torun Law Office, we have an excellently skilled team of lawyers experienced first and foremost in Data Protection Law, Administrative jurisdiction, Arbitrations and Mediations, Human Rights and Humanitarian Law, Trade Law, Construction Law, Labor and Social Security Law, International Private Law, procedures and lawsuits regarding the Military personnel as well as the fields listed below.

Our aim is to deliver justice to those in need within the framework of law as an attorney in the current judicial system in accordance with the principles of integrity and honesty.
With our current team we offer legal services in the following fields;

- Criminal Law
- Law of Obligations
- Family Law
- Execution and Bankruptcy Law
- Consumer Law
- Real-estate Law and Condominium Law

**Önceliğimiz Etik Değerlere,
İnsan Haklarına Saygı ve İş Disiplini
Our Priority is Respect for Ethical Values,
Human Rights and Work Discipline**

TORUN HUKUK BÜROSU

torunhukukburosu@gmail.com

Cevizlidere Mah. 1219. Sok.
No:2 Latif Apt.D.3 Balgat
06520 Çankaya/ANKARA

Telefon : 0 312 432 56 78
Mobil : 0 553 707 43 26