Esin Attorney Partnership.

Amendments to the Turkish Data Protection Law

Amendments to the Turkish Data Protection Law

Processing of sensitive personal data

RULE:
Processing of sensitive personal data is prohibited.

EXCEPTIONS:

- (a) Explicit consent
- (b) Explicitly stipulated by laws
- (c) Processing is necessary to protect the life or physical integrity of the data subject or of another natural person where the data subject cannot disclose their consent due to actual impossibility or whose consent is not legally valid
- (ç) Processing of personal data made public, in accordance with the intention of the data subject
- (d) Processing is mandatory for the establishment exercise or protection of a right
- (e) Processing by persons or authorized institutions and organizations under the obligation of confidentiality, for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and for the planning, management and financing of health services
- (f) Processing mandatory for the fulfillment of legal obligations in the field of employment, occupational health and safety, labor and social security or social services and social assistance
- (g) Processing carried out by other non-profit organizations established for political, philosophical, religious or trade union purposes on condition that the processing relates solely to the members of the organization or to persons who are in regular contract with this organization

Cross-border Transfer of Personal Data

Rule:
Presence of **legal grounds set out in Articles 5 and 6 of the LPPD**
+
Existence of an adequacy decision issued by the Board that the third country, sector within the third country or international organizations to which personal data will be transferred provides adequate protection

in the absence of

adequacy decision

Presence of **legal set out in Articles 5 and 6 of the LPPD**
+
Data subject having the **opportunity to exercise their rights and to apply for effective remedies** in the recipient country
+
Fulfillment of the following **safeguards**

- (a) Existence of an agreement that does not constitute an international contract between (i) public institutions and organizations or international organizations abroad, and (ii) public institutions and organizations professional association with public entity status in Türkiye
  +
  Board's permission
- (b) Existence of binding corporate rules for companies within a group of undertakings engaged in joint economic activity
  +
  Board's approval
- (c) Existence of standard contractual clauses published by the Board
  +
  notification to the Authority within 5 business days
- (ç) Existence of a written undertaking containing provisions to ensure adequate protection
  +
  Board's permission

in the absence of

appropriate safeguards

Exceptions for occasional cases

- (a) Data subject's explicit consent to the transfer, provided that they have been informed about the potential risks
- (b) Transfer is being necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject
- (c) Transfer is being necessary for the establishment or performance of a contract between the data controller and another natural or legal person for the benefit of the data subject
- (ç) Transfer is being necessary for an overriding public interest
- (d) Transfer is being necessary for the establishment, exercise or protection of a right
- (e) Transfer is being necessary to protect the life or physical integrity of the data subject or of another natural person where the data subject cannot disclose their consent due to actual impossibility or whose consent is not legally valid
- (f) Transfer is being made from a register that is open to the public or persons with a legitimate interest, to the extent that the conditions laid down by applicable law for accessing the registry is met and transfer is requested by those having legitimate interest.

Abbreviations	
"LPPD"	Law No. 6698 on the Protection of Personal Data
"Authority"	Data Protection Authority
"Board"	Data Protection Board

Effective Date

Amendments
The amendments to the Law on the Protection of Personal Data ("**LPPD**") will enter into force on June 1, 2024.

Our Comments and Potential Effects
Within the scope of the amendments, new mechanisms are stipulated, especially for cross-border transfers. In order for these mechanisms to be implemented, the Personal Data Protection Authority ("**Authority**") is expected to publish the standard contractual clauses and provide guidance and actions to clarify how these mechanisms will work together with the existing transfer mechanisms.

Processing of Sensitive Personal Data

Amendments
The amendments introduce new and alternative legal grounds for the processing of sensitive personal data under the LPPD.

Accordingly, the processing of sensitive personal data will only be allowed if one of the following legal grounds is relied upon:

i. *The explicit consent of the data subject;*

ii. *It is expressly stipulated by law*

Example: Processing of data on criminal convictions in accordance with the Law No. 5352 on Judicial Records; collection of people's fingerprints in accordance with Article 5 of the Law No. 2559 on Police Duties and Powers

iii. *Processing is necessary to protect the life or physical integrity of the data subject or of another natural person where the data subject cannot disclose their consent due to actual impossibility or whose consent is not legally valid;*

Example: Processing of sensitive personal data such as blood type and previous illnesses for the purpose of protecting the life or bodily integrity of a person who is unable to disclose their consent due to loss of consciousness for any reason

iv. *Processing of personal data made public by the data subject in accordance with the intention of the data subject;*

Example: Processing and use of personal data such as blood type and allergy information that a person has shared in a publicly accessible environment for use in emergencies, provided that the processing is in accordance with such purpose

v. *Processing is mandatory for the establishment, exercise or protection of a right;*

Example: Ongoing retention by employers of the health data of their former employees in order to exercise their defence rights in lawsuits that may be filed after the termination of the employment contract; processing of a disabled person's disability report by the tax office in order for a disabled person to benefit from the right to purchase a vehicle by being exempt from special consumption tax

vi. *For the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and for the planning, management and financing of health services, processing by persons or authorized institutions and organizations under the obligation of confidentiality;*

Example: Data and records kept by the Ministry of Health and all kinds of health institutions and the Social Security Institution for the purposes set out in this subparagraph

vii. *Processing is mandatory for the fulfilment of legal obligations in the field of employment, occupational health and safety, labour and social security or social services and social assistance*

Example: Processing of individuals' health data or criminal conviction data by employers in order to fulfil the obligation to employ disabled or convicted persons as per the Labour Law No. 4857; processing of the person's health report in order to fulfil the transportation service to health institutions provided to dialysis patients

viii. *Processing of personal data of current or former members of foundations, associations or other non-profit organizations established for political, philosophical, religious or trade union purposes, or persons who are in regular contact with these organizations and formations under certain conditions.*

Example: Processing of information about current members of such organizations and entities, as well as former members and persons who are in regular contact with them by making donations; processing by a trade union of data relating to its field of activity and purpose only on trade union membership (however, personal data relating to the health or religion of trade union members cannot be processed as it is not related to its field of activity and purpose)

Our Comments and Potential Effects

The categories for sensitive personal data have been retained as is under Article 6 of the LPPD. However, obtaining explicit consent is no longer appears as the main rule and explicit consent is now listed as an option among other legal grounds for processing of sensitive personal data.

The amendments eliminate the binary distinction between the exceptions for sensitive personal data relating to health and sexual life and other sensitive personal data. In this respect, it is possible to say that the regulation is in line with Article 9 of the European General Data Protection Regulation ("**GDPR**").

Accordingly, it is now possible for data controllers to process sensitive personal data based on new mechanisms without obtaining explicit consent, especially for employment and occupational health and safety processes. Therefore, explicit

consent may not be required in all cases for the processing of sensitive personal data of employees and that employee privacy notices may need to be revised accordingly in the future.

However, unlike the GDPR, the requirement of "expressly provided by law", which is stipulated in the previous version of the LPPD, is also preserved.

Nevertheless, unlike the amendments, the GDPR also includes "public interest" and "processing of sensitive personal data for archiving, scientific or historical research and statistical purposes within the scope of public interest" as processing grounds. Although such legal grounds are not specifically listed under Article 6 among the options in the LPPD, please note that the anonymous processing of personal data for research, planning and statistical purposes is subject to a general exception pursuant to Article 28 of the LPPD.

In the amendments, the requirement to take adequate measures determined by the Personal Data Protection Board ("**Board**") for the processing of sensitive personal data in the existing Article 6 is preserved.

Cross-Border Transfer of Personal Data

Amendments

With the amendments, comprehensive changes have been made to cross-border data transfer mechanisms. A tiered system is envisaged for personal data transfers abroad:

1. Existence of an adequacy decision:

   Presence of legal grounds set out in Articles 5 and 6 of the LPPD

   +

   The existence of an adequacy decision issued by the Board that the third country, sector within the third country or international organization to which personal data will be transferred provides adequate protection

2. In the absence of an adequacy decision:

   Presence of legal grounds set out in Articles 5 and 6 of the LPPD

   +

   data subject having the opportunity to exercise their rights and to apply for effective remedies in the recipient country

   +

   Fulfilment of the following safeguards specified in the LPPD

i. *Existence of an agreement (which is not an international contract) between public institutions and organizations abroad or international organizations, and public institutions and organizations or professional association with public entity status in Türkiye + Board's permission*

ii. *Existence of binding corporate rules for companies within a group of undertakings engaged in joint economic activity + Board's approval*

iii. *Existence of standard contractual clauses published by the Board + notification to the Authority within 5 business days*

iv. *Existence of a written undertaking containing provisions to ensure adequate protection + Board's permission*

3. In the absence of an adequacy decision and appropriate safeguards

In cases where there is no adequacy decision and appropriate safeguards cannot be provided, it is stipulated that personal data may be transferred abroad in the following cases, provided that it is occasional:

i. *The data subject's explicit consent to the transfer, provided that they have been informed about the potential risks*

ii. *The transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject*

iii. *The transfer is necessary for the establishment or performance of a contract between the data controller and another natural or legal person for the benefit of the data subject*

iv. *The transfer is necessary for an overriding public interest*

v. *The transfer is necessary for the establishment, exercise or protection of a right*

vi. *The transfer is necessary to protect the life or physical integrity of the data subject or of another natural person where the data subject cannot disclose their consent due to actual impossibility or whose consent is not legally valid*

vii. *The transfer is made from a register that is open to the public or persons with a legitimate interest, to the extent that the conditions laid down by applicable law for accessing the registry and transfer is requested by those having legitimate interest are met*

The amendments acknowledges onward transfers for the first time legally and sets out that onwards transfers are subject to cross-border transfer rules.

The amendments sets out a transition period in relation to cross-border transfers based on explicit consent. In this context, data controllers that obtain explicit consent for cross-border transfer can continue to rely on these explicit consents till September 1, 2024.

Finally, it is stated that the principles and procedures on cross-border transfers will be regulated by a regulation.

Our Comments and Potential Effects
Significant amendments are envisaged for the existing Article 9. A structure similar to the GDPR is established by the amendments, namely (i) the existence of an adequacy decision, (ii) the provision of appropriate safeguards in the absence of an adequacy decision, and (iii) the cases in the absence of an adequacy decision and appropriate safeguards.

However, unlike the GDPR, the amendments also require that the transfers in these cases must also be "occasional" in terms of the transfer mechanisms specified for cases where both an adequacy decision and adequate safeguards are absent. Continuous transfers therefore require an adequacy decision or appropriate safeguards in the recipient country.

The amendments are particularly important for the transfer processes that are currently being relied on explicit consent. With the amendments, explicit consent is now considered as an exceptional mechanism for the cross-border transfer of personal data. Hence, data controllers who currently transfer personal data abroad relying on explicit consent shall review their transfer processes.

Pursuant to the transitional provision, explicit consents obtained before or after the entry into force of Article 9, based on the pre-amended version of Article 9 will remain valid until September 1, 2024. Therefore, for the sake of managing the transition period, it is made possible for explicit consents obtained before the amendment to be valid for three months. However, no such provision has been introduced for the already approved undertaking letters. Therefore, one may argue that transfers made on the basis of these undertaking letters may continue.

The amendments do not regulate in detail how other existing mechanisms, such as undertaking letters, will operate in conjunction with the new mechanisms and the publication of the standard contractual clauses. It is foreseen that these issues will be shaped by the additional legislation of the Authority such as announcements and regulations before September 1, 2024, when explicit consents will cease to be valid.

Standard Contractual Clauses

Amendments
Pursuant to the amendments introduced to Article 9, data controllers and data processors must notify the Authority that they have signed standard contractual clauses within 5 days as of signing. Failure to notify may result in administrative fines up to TRY 1 million.

Our Comments and Potential Effects
With this amendment, for the first time in the LPPD, the notification regarding the signing of the standard contractual clauses has been deemed sufficient, and a mechanism that does not require the approval of the Authority has been introduced.

Further, the amendments enable the imposition of administrative fines on data processors as well, in case of failure to notify the signing of the standard contractual clauses

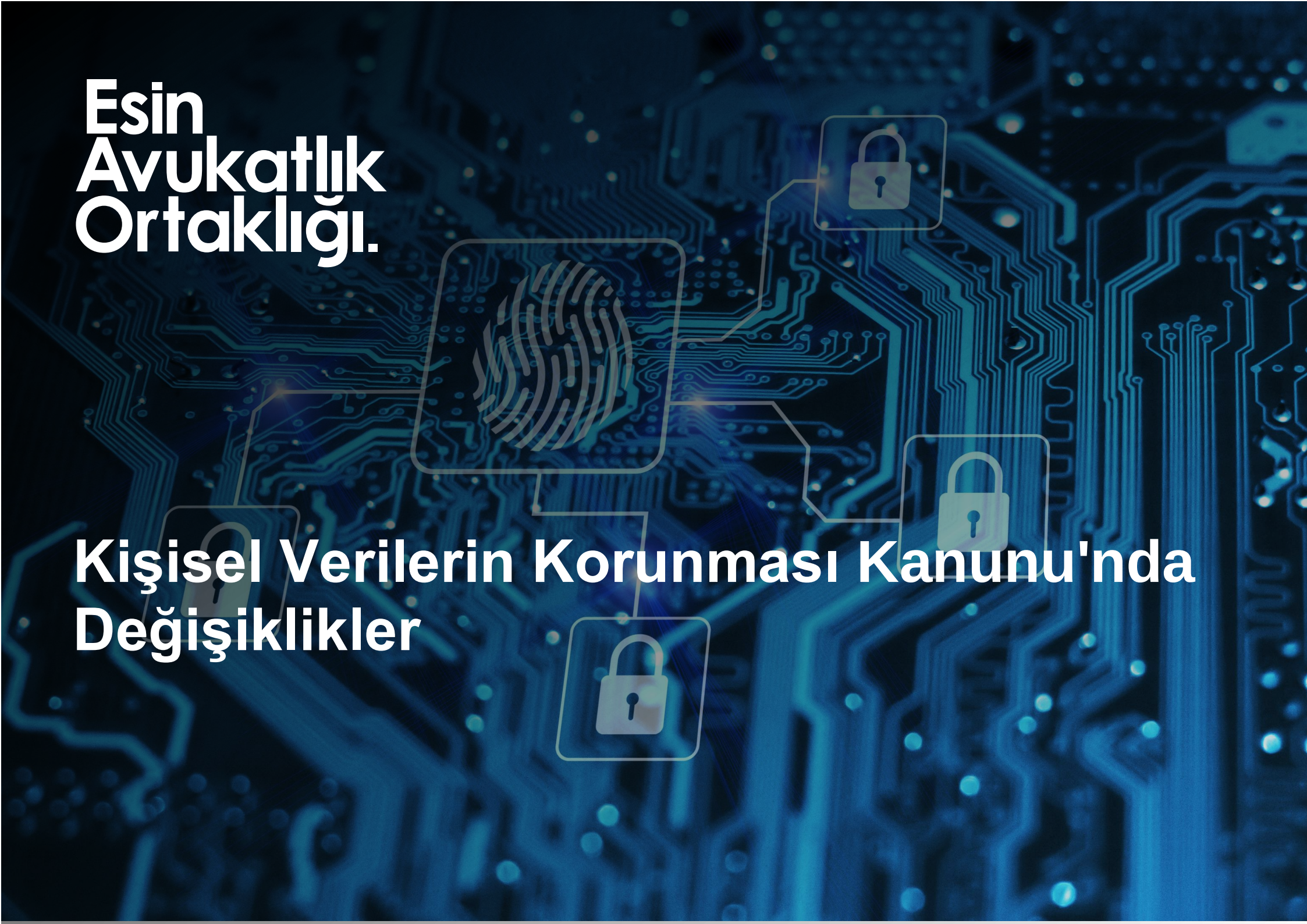
Appeal

Amendments
Administrative courts are determined as the sole judicial authority for appeals against administrative fines imposed for violations of the LPPD. However, applications pending before criminal judgeships of peace as of June 1, 2024, the effective date of the amendments, will continue to be heard by these judgeships.

Our Comments and Potential Effects
Before the amendments, the appeal process against the administrative fines imposed by the Authority was subject to the appeal procedure regulated under the Misdemeanors Law, and therefore, the criminal judgeships of peace were set out as the appeal authority. However, pursuant to the amendments, criminal judgeships of peace will no longer be authorized for appeal. Accordingly, appeals against administrative fines imposed by the Board will be subject to the 60-day period applicable to administrative appeals, instead of the 15-day appeal period before the criminal judgeships of peace.

Esin
Avukatlık
Ortaklığı.

Kişisel Verilerin Korunması Kanunu'nda Değişiklikler



Kişisel Verilerin Korunması Kanunu'nda Değişiklikler

Özel Nitelikli Kişisel Verilerin İşlenmesi

KURAL:
Özel nitelikli kişisel verilerin işlenmesi yasaktır.

İSTİSNALAR:

- (a) Açık rıza
- (b) Kanunlarda açıkça öngörülmesi
- (c) Fiili imkansızlık nedeniyle rızasını açıklayamayacak veya rızasına hukuki geçerlilik tanınmayan kişilerin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması
- (ç) Alenileştirilen kişisel verilere ilişkin ve alenileştirme iradesine uygun olması
- (d) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
- (e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili otoritelerce, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması
- (f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması
- (g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan kar amacı gütmeyen oluşumlar tarafından; mevcut veya eski üyeleri ve mensupları ile bu kuruluş ve oluşumlarla düzenli temasta olan kişilerin verilerinin işlenmesi

Kişisel Verilerin Yurt Dışına Aktarılması

KURAL:
KVKK'nın 5. ve 6. maddesinde yer alan hukuki sebeplerin mevcut olması
+
Kişisel verilerin aktarılacağı üçüncü ülke, ülkedeki sektör ya da uluslararası kuruluşun yeterli korumayı sağladığına ilişkin Kurul tarafından verilen yeterlilik kararının bulunması

yeterlilik kararı

yoksa

KVKK'nın 5. ve 6. maddesinde yer alan hukuki sebeplerin mevcut olması
+
İlgili kişinin aktarımın yapılacağı ülkede haklarını kullanma ve kanun yollarına başvurma imkanının bulunması
+
Aşağıdaki güvencelerden birinin sağlanması

- (a) (i) Yabancı kamu otoriteleri veya uluslararası kuruluşlar ile (ii) Türkiye'deki kamu otoriteleri veya kamu kurumu niteliğindeki meslek kuruluşlar arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı
  +
  Kurul izni
- (b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketler bakımından, bağlayıcı şirket kurallarının varlığı
  +
  Kurul onayı
- (c) Kurul tarafından ilan edilmiş standart sözleşmelerin varlığı
  +
  5 işgünü içinde Kurum'a bildirim
- (ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı
  +
  Kurul izni

güvenceler

yoksa

Arızi olmak kaydıyla istisnalar

- (a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi
- (b) Aktarımın, ilgili kişiyle veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması
- (c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması
- (ç) Aktarımın üstün bir kamu yararı için zorunlu olması
- (d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması
- (e) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik bulunmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması
- (f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati bulunan kişinin talep etmesi kaydıyla aktarım yapılması

Kısaltmalar	
"KVKK"	6698 sayılı Kişisel Verilerin Korunması Kanunu
"Kurum"	Kişisel Verileri Koruma Kurumu
"Kurul"	Kişisel Verileri Koruma Kurulu

Yürürlük Tarihi

Değişiklikler
Kişisel Verilerin Korunması Kanunu'nda ("**KVKK**") yapılması öngörülen değişiklikler, 1 Haziran 2024 tarihi itibarıyla yürürlüğe girecektir.

Yorumlar ve Olası Etkiler
Değişiklikler kapsamında özellikle yurt dışına aktarım süreçleri bakımından yeni mekanizmalar öngörülmektedir. Bu mekanizmaların işlemesi için Kişisel Verileri Koruma Kurumu'nun ("**Kurum**") standart sözleşme maddelerini yayımlaması ve söz konusu mekanizmaların var olan aktarım mekanizmaları ile birlikte nasıl işleyeceğini netleştirmesi için yönlendirme ve aksiyonları beklenmektedir.

Özel Nitelikli Kişisel Verilerin İşlenmesi

Değişiklikler

Değişiklikler, KVKK kapsamındaki özel nitelikli kişisel verilerin işlenmesine ilişkin yeni ve alternatif hukuki sebepler öngörmektedir.

Buna göre, özel nitelikli kişisel verilerin işlenmesi ancak aşağıdaki hukuki sebeplerden birine dayanılması halinde mümkün olacaktır:

i. *ilgilinin açık rızasının bulunması;*

ii. *kanunlarda açıkça öngörülmesi;*

Örnek: 5352 sayılı Adli Sicil Kanunu uyarınca ceza mahkumiyetine ilişkin verilerin işlenmesi; 2559 Polis ve Vazife ve Salahiyet Kanununun 5 inci maddesi uyarınca kişilerin parmak izlerinin alınması

iii. *fiili imkansızlık sebebiyle rızasını açıklayamayacak ya da rızasına hukuki geçerlilik tanınamayacak kişilerin kendisinin ya da bir başkasının hayatı ve beden bütünlüğünün korunması için zorunlu olması;*

Örnek: Herhangi bir sebeple bilinç kaybından ötürü rızasını açıklayamayacak durumda olan kişinin hayatının veya beden bütünlüğünün korunması amacına mahsus olarak kan grubu ve geçirilen hastalıklar gibi özel nitelikli kişisel verilerin işlenmesi

iv. *ilgili kişilerin alenileştirdiği kişisel verilerin alenileştirme amacına uygun işlenmesi;*

Örnek: Bir kişinin acil durumlarda kullanılması için, herkesçe erişilebilir bir alanda paylaşmış olduğu kan grubu ve alerji bilgileri gibi kişisel verilerinin bu amaca uygun olarak işlenmesi ve kullanılması

v. *bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması;*

Örnek: İş sözleşmesinin sona ermesinden sonra açılması muhtemel davalarda savunma hakkının kullanılması bakımından işverenin eski işçisine ait sağlık verilerini saklamaya devam etmesi; engelli bir kişinin özel tüketim vergisinden istisna olarak araç alma hakkından yararlanabilmesi için bu kişinin engelli raporunun vergi dairesi tarafından işlenmesi

vi. *kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi;*

Örnek: Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun bu bentte yazılı amaçlarla tuttukları veriler ve kayıtlar

vii. *istihdam, iş sağlığı ve güvenliği, iş ve sosyal güvenlik veya sosyal hizmetler ile sosyal yardım alanındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması;*

Örnek: 4857 sayılı İş Kanunuyla işverenlere verilen engelli veya hükümlü çalıştırma yükümlülüğünün yerine getirilebilmesi bakımından kişilerin sağlık verilerinin veya ceza mahkumiyetine ilişkin verilerinin işverenlerce işlenmesi; diyaliz hastalarına sunulan sağlık kuruluşlarına taşıma hizmetinin yerine getirilebilmesi için kişinin sağlık raporunun işlenmesi

viii. *siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek veya diğer kar amacı gütmeyen oluşumların belirli koşullar altında mevcut veya eski üyelerine ve mensuplarına yahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik kişisel verilerin işlenmesi.*

Örnek: Söz konusu kuruluş ve oluşumların mevcut üyelerinin yanı sıra eski üyeleri ve düzenli olarak bağış yapmak suretiyle kendisiyle temas halinde olan kişilerin bu durumlarına ilişkin bilgiyi işlemesi; bir sendikanın kendi faaliyet alanına ve amacına ilişkin olarak sadece sendika üyeliğiyle ilgili verileri işlemesi (ancak sendika üyelerinin sağlık veya dinine yönelik kişisel veriler, faaliyet alanıyla ve amacıyla ilgisi olmaması sebebiyle işlenemez)

Yorumlar ve Olası Etkiler

KVKK'nın 6. maddesinde sayılan özel nitelikli kişisel veri kategorileri eski haliyle muhafaza edilmektedir. Ancak, özel nitelikli kişisel verilerin işlenmesi için açık rıza alınması yönündeki ana kurala ilişkin hüküm kaldırılarak, açık rıza diğer veri işleme şartları arasında bir seçenek olarak sayılmaktadır.

Değişiklikler ile sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerle, diğer özel nitelikli kişisel verilerin faydalanacağı istisnalara ilişkin ikili ayrım ortadan kaldırılmaktadır. Bu yönüyle düzenlemenin Avrupa Genel Veri Koruma Tüzüğü'nün ("**GDPR**") 9. maddesine paralel şekilde düzenlendiğini söylemek mümkündür.

Bu doğrultuda, artık, özellikle de istihdam ve iş sağlığı güvenliği süreçleri bakımından veri sorumlularının açık rıza almaksızın yeni mekanizmalara dayanarak özel nitelikli kişisel verileri işlemesinin önü açılmıştır. Dolayısıyla, çalışanların özel nitelikli kişisel verilerinin işlenmesi bakımından her durumda açık rıza gerekmeyebileceği ve ilerleyen süreçte çalışan aydınlatma metinlerinin bu kapsamda gözden geçirilmesinin faydalı olacağı kanaatindeyiz

Ancak, GDPR'dan farklı olarak, KVKK'nın mevcut halinde öngörülmüş olan "kanunlarda açıkça öngörülmesi" şartı da muhafaza edilmektedir.

Bununla beraber, GDPR, değişikliklerden farklı olarak "kamu yararını" ve "kamu yararı kapsamında arşivleme, bilimsel veya tarihi araştırma ve istatistiksel amaçlarla özel nitelikli kişisel veri işlenmesini de şartlar arasında saymaktadır. KVKK'da getirilen seçenekler arasında bu hukuki sebep 6. madde kapsamında özellikle belirtilmemiş olsa da, araştırma, planlama ve istatistik sebepleriyle kişisel verilerin anonim olarak işlenmesinin KVKK'nın 28. maddesi uyarınca genel bir istisnaya tabi olduğunu hatırlatmak isteriz.

Değişikler kapsamında, ayrıca, mevcut 6. maddedeki özel nitelikli kişisel verilerin işlenmesinde ayrıca Kişisel Verileri Koruma Kurulu ("**Kurul**") tarafından belirlenen yeterli önlemlerin alınması şartı korunmaktadır.

Kişisel Verilerin Yurt Dışına Aktarılması

Değişiklikler

Değişiklikler ile, yurt dışına veri aktarım mekanizmalarında kapsamlı düzenlemeler yapılmıştır. Yurt dışına kişisel veri aktarımları için kademeli bir sistem öngörülmektedir:

1. Yeterlilik kararı bulunması:

   KVKK'nın 5. ve 6. maddesinde yer alan hukuki sebeplerin mevcut olması

   +

   Kişisel verilerin aktarılacağı üçüncü ülke, ülkedeki sektör ya da uluslararası kuruluşun yeterli korumayı sağladığına ilişkin Kurul tarafından verilen yeterlilik kararının bulunması

2. Yeterlilik kararı bulunmaması:

KVKK'nın 5. ve. 6. maddesinde yer alan hukuki sebeplerin mevcut olması

+

ilgili kişinin aktarımın yapılacağı ülkede haklarını kullanma ve kanun yollarına başvurma imkanının bulunması

+

KVKK'da yer alan aşağıdaki güvencelerin sağlanması

i. *Yabancı kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı + Kurul izni*

ii. *Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketler bakımından, bağlayıcı şirket kurallarının varlığı + Kurul onayı*

iii. *Kurul tarafından ilan edilmiş standart sözleşmelerin varlığı + 5 işgünü içinde Kurum'a bildirim*

iv. *Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı + Kurul izni*

3. Yeterlilik kararı ve güvencelerin bulunmaması

Yeterlilik kararı bulunmayan ve söz konusu güvencelerin sağlanamadığı hallerde ise, arızi olmak kaydıyla, aşağıdaki durumlarda kişisel verilerin yurt dışına aktarılabileceği öngörülmektedir:

i. *İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi*

ii. *Aktarımın, ilgili kişiyle veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması*

iii. *Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması*

iv. *Aktarımın üstün bir kamu yararı için zorunlu olması*

v. *Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması*

vi. *Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik bulunmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması*

vii. *Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati bulunan kişinin talep etmesi kaydıyla aktarım yapılması*

Değişiklikler ile, devam eden aktarıma ilişkin düzenlemeler ilk defa hüküm altına alınmakta ve devam eden aktarımların kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlere tabi olacağı düzenlenmektedir.

Değişiklikler, açık rızaya dayalı yurt dışına kişisel veri aktarımları bakımından bir geçiş süreci öngörmektedir. Bu kapsamda, yurt dışına kişisel veri aktarımları için açık rızaya dayanan veri sorumluları, 1 Eylül 2024 tarihine kadar mevcut açık rızalara dayalı olarak veri aktarmaya devam edebilecektir.

Son olarak, kişisel verilerin yurt dışına aktarılması ile ilgili esas ve usullerin yönetmelik ile düzenleneceği belirtilmektedir.

Yorumlar ve Olası Etkiler

Mevcut 9. madde önemli değişiklikler öngörülmektedir. GDPR ile benzer şekilde (i) yeterlilik kararının bulunması, (ii) yeterlilik kararı bulunmadığı hallerde yeterli güvencelerin sağlanması ve (iii) yeterlilik kararının ve yeterli güvencelerin bulunmadığı haller olmak üzere kademeli bir yapı oluşturulmaktadır.

Ancak değişikliklerde, yeterlilik kararının ve yeterli güvencenin bulunmadığı haller için belirtilen aktarım mekanizmaları bakımından, GDPR'dan farklı olarak, bu hallerdeki aktarımların aynı zamanda "arızi" olması şartı da aranmaktadır. Dolayısıyla devamlı olarak gerçekleştirilecek aktarımlar için, yeterlilik kararı veya aktarım yapılacak ülkede yeterli güvencelerin bulunması gerekmektedir.

Değişiklikler, özellikle, mevcut düzende açık rızaya dayalı olarak kurulan aktarım süreçleri açısından önem arz etmektedir. Değişiklikler ile birlikte, açık rıza artık yurt dışına kişisel verilerin aktarılması bakımından istisnai bir mekanizma olarak karşımıza çıkmaktadır. Bu nedenle, halihazırda açık rızaya dayalı olarak yurt dışına kişisel veri aktarımı gerçekleştiren veri sorumlularının aktarım süreçlerini gözden geçirmesi gerekmektedir.

Düzenlenen geçiş hükmü uyarınca, 9. maddenin değişiklikten önceki 1. fıkrası kapsamında, madde yürürlüğe girmeden evvel ya da sonrasına alınan açık rızalar 1 Eylül 2024 tarihine kadar geçerliliğini koruyacaktır. Böylece geçiş sürecinin yönetilebilmesi adına değişiklikten önce alınan açık rızaların üç ay süreyle geçerli olması mümkün kılınmıştır. Ancak halihazırda onaylanan taahhütnameler ile ilgili bu yönde bir düzenleme getirilmemiştir. Dolayısıyla, bu taahhütnamelere dayanılarak yapılan aktarımlara devam edilebileceği söylenebilir.

Taahhütnameler gibi halihazırda var olan mekanizmaların, yeni getirilen mekanizmalarla birlikte nasıl işleyeceği, standart sözleşme hükümlerinin yayımlanma zamanı gibi hususlar ise değişikliklerde detaylı olarak düzenlenmemektedir. Bu hususların, açık rızaların geçerliliğini yitireceği 1 Eylül 2024 tarihinden önce Kurum'un duyuru, yönetmelik gibi ilave çalışmaları ile şekillenmesi yönünde beklentiler büyümektedir.

Standart Sözleşme Hükümleri

Değişiklikler

Veri sorumluları ve veri işleyenlerin, 9. maddeye getirilen değişiklikler uyarınca, standart sözleşme hükümlerini imzalamalarını takip eden 5 gün içerisinde Kurum'a bildirimde bulunmaları gerekmektedir. Bildirim yükümlülüğünün yerine getirilmemesi halinde 1 milyon TL'ye kadar idari para cezası öngörülmektedir.

Yorumlar ve Olası Etkiler

Söz konusu değişiklik ile, KVKK'da ilk kez, standart sözleşme hükümlerinin imzalandığına ilişkin bildirim yeterli görülmüş ve Kurum onayını gerektirmeyen bir mekanizmanın önü açılmıştır.

Ayrıca ilgili düzenleme ile, standart sözleşme hükümlerinin imzalandığına ilişkin bildirim yükümlülüğünün ihlali halinde veri işleyenlere yönelik idari para cezası uygulanması imkanı doğmaktadır.

İtiraz

Değişiklikler

KVKK'ya aykırılık nedeniyle verilen idari para cezası kararlarına karşı itirazlar bakımından idare mahkemeleri tek yargı mercii olarak belirlenmektedir. Ancak değişikliklerin yürürlük tarihi olarak belirlenen 1 Haziran 2024 tarihi itibarıyla sulh ceza hakimliklerinde görülmekte olan başvurular, bu hakimliklerce görülmeye devam edilecektir.

Yorumlar ve Olası Etkiler

Değişiklikler öncesinde, Kurum tarafından verilen idari para cezalarına itiraz süreci, Kabahatler Kanunu kapsamında düzenlenen itiraz usulüne tabi olduğundan, itiraz mercii olarak sulh ceza hakimliklerine başvurulmaktaydı. Değişiklikler uyarınca, sulh ceza hakimlikleri artık itiraz mercii olarak yetkili olmayacaktır. Bu doğrultuda, Kurul tarafından verilen idari para cezalarına itirazlar, sulh ceza hakimlikleri nezdindeki 15 günlük itiraz süresi yerine, idari itirazlara ilişkin 60 günlük süreye tabi olacaktır.