DL | Avukatlık Bürosu

’Kişisel verilerin korunması: Bilinmesi gerekenler‘

Yönetici Özeti 1
1.Genel Olarak Kişisel Verilerin Korunması ve Korunan Hukuki Değer 2
2.Kişisel Veri 4
3.Özel Nitelikli Kişisel Veri 5
4.Kişisel Verilerin Korunması ile İlgili Genel İlkeler 6
5.Kişisel Verilerin İşlenme Şartları 8
6.Özel Nitelikli Kişisel Verilerin İşlenme Şartları 10
7.Kişisel Verilerin Aktarılması 11
8.Veri Sorumlusunun Yükümlülükleri 12
9.İlgili Kişinin Hakları 15
10.Veri Sorumlusuna Başvuru ve Şikâyet Mekanizması 16
11.Kişisel Verilerin Korunması Kurumu ve Kişisel Verilerin Korunması Kurulu 18
12.Yaptırımlar 20
13. Mahremiyet Etki Analizi ve Alınması Gereken Aksiyonlar 23

Yönetici Özeti

24 Mart 2016 tarihinde kabul edilmiş, 7 Nisan 2016 tarihinde 29677 sayılı Resmi Gazetede yayımlanmış olan 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında detaylıca incelenen **'Kişisel verilerin korunması: Bilinmesi gerekenler'** adını verdiğimiz çalışmamızı sizlerle paylaşmaktan mutluluk duyarız. Kişisel veriler ilerleyen sayfalarda detaylı olarak belirtildiği gibi, bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak tanımlanmaktadır. Günümüzde söz konusu veriler gerek özel gerekse kamu sektörlerinde kullanılmaktadır. Bu durum bireyler ile mal ve hizmet sunanlar bakımından bir takım avantajlar sağlasa da, kişisel verilerin istismar edilme riskini de beraberinde getirmektedir. Dolayısıyla, doğabilecek olası riskleri bertaraf etmek adına şirketlerin ve kurumların bu konuda önlem almaları uygun olacaktır.

Bu çalışmamızda;

- Genel olarak kişisel verilerin korunması ve korunan hukuki değer,
- Kişisel veri tanımı,
- Özel nitelikli kişisel veri tanımı,
- Kişisel verilerin korunması ile ilgili genel ilkeler,
- Kişisel verilerin işlenme şartları,
- Özel nitelikli kişisel verilerin işlenme şartları,
- Kişisel verilerin üçüncü kişilere ve yurt dışına aktarılması,
- Veri sorumlusunun yükümlülükleri,
- İlgili kişinin hakları,
- Veri sorumlusuna başvuru ve şikâyet mekanizması,
- Kişisel verilerin korunması kurumu ve kişisel verilerin korunması kurulu,
- Suçlar ve kabahatler ile ilgili yaptırımlar,

ile ilgili genel bir bilgi verilmiş olup, şirketlerin bu hususta doğabilecek risklerini tespit etmelerini sağlamak ve alınabilecek önlemlerin saptanabilmesini kolaylaştırmak amaçlanmıştır.

Yeni bir düzenleme olan Kişisel Verilerin Korunması Kanunu'nun getirdiklerine dair kılavuz niteliğinde olacağına inandığımız bu çalışmamızın sizler için faydalı olmasını umuyoruz.

1. Genel olarak kişisel verilerin korunması ve korunan hukuki değer

6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVK", "Kanun") 24 Mart 2016 tarihinde kabul edilmiş, 7 Nisan 2016 tarihinde Resmi Gazetede yayımlanmıştır. Kanun'un yayım tarihinden önce işlenmiş olan kişisel verilerin, yayım tarihinden itibaren iki yıl içinde Kanun hükümlerine uygun hale getirilmesi zorunlu tutulmuştur. Kanun'un yayım tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması halinde Kanun'a uygun kabul edileceklerdir. Kanun'da ayrıca bir takım yönetmeliklerin yürürlüğe gireceği öngörülmüş olup söz konusu yönetmelikler Kanun'un yayım tarihinden itibaren bir yıl içerisinde yürürlüğe konulacaktır.
Aşağıda detaylı olarak açıklanacak olan, üçüncü kişilere ve yurt dışına aktarma, ilgilinin hakları, ilgilinin başvurusuna yanıt verme yükümlülüğü, Kurul'a şikâyet, Re'sen inceleme, Veri Sorumluları Sicili ile suçlar ve kabahatlerin düzenlendiği hükümler, Kanun'un yayım tarihinden itibaren 6 aylık sürenin sonunda yürürlüğe girecektir.
Kanun'un 1. maddesi uyarınca amacı kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.
Kanun'un 2. maddesinde kapsamının 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 uygulanacağı hükme bağlanmıştır.
Anayasa'nın 20.maddesine 2010 yılında yapılmış olan değişiklik ile 'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla

işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.' hükmü eklenmiştir. KVK'nın 1. maddesinin gerekçesinde de Kanun'un amacının kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasa'da öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlükleri korumak olduğu belirtilmiştir. Ayrıca yine madde gerekçesinde, kişinin mahremiyet hakkı ile bilgi güvenliği hakkının da KVK kapsamında koruma altına alınmak istendiği belirtilmiştir.

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde de 'Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.' hükmü yer almaktadır.

Son olarak Türk Ceza Kanunu'nun ("TCK") 135 ila 140. maddelerinde aşağıda detaylı olarak incelenecek olan kişisel verilere ilişkin suçlar düzenlenmiştir. Söz konusu suçlar TCK'da Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığının altında düzenlenmiş olup korunan hukuki değerin özel hayatın gizliliği olduğu anlaşılmaktadır.

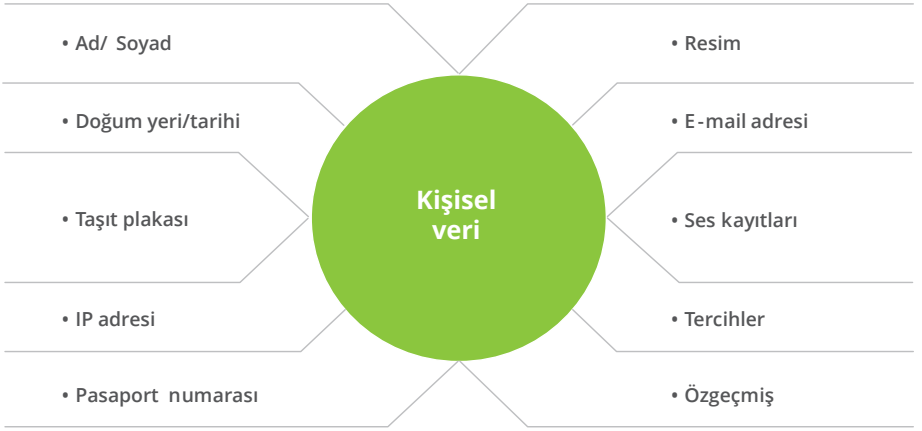
Kişisel verilerin korunması –Şirkete faydaları

2.Kişisel veri

"Kişisel Veri", KVK'nın 3. maddesinde kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Anayasa Mahkemesi, kişisel verileri kişinin adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, SGK numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler olarak tanımlamıştır.[1]
KVK'nın madde gerekçesinde de kişisel verinin, bireyin kesin teşhisini sağlayan bilgiler olabileceği gibi; aynı zamanda, kişi ile ilişkilendirilebilecek ve bu surette o kişinin belirlenmesini, tanınmasını sağlayan verileri de kapsayacağı belirtilmiştir.

Tüzel kişilere ilişkin kişisel veriler bu tanımın kapsamına girmemektedir. Dolayısıyla tüzel kişilerin unvanı ya da adresi gibi bilgiler herhangi bir gerçek kişi ile ilişkilendirilmediği sürece kişisel veri sayılmayacaktır.

"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi



[1]Anayasa Mahkemesi E. 2013/122 K. 2014/74, 09.04.2014

3. Özel nitelikli kişisel veri

Başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikle olan ve bu nedenle daha fazla korumaya ihtiyaç duyulan kişisel verilere özel nitelikli kişisel veri denmektedir.

Özel nitelikli kişisel verilerin kapsamına 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 girmektedir.

4. Kişisel verilerin korunması ile ilgili genel ilkeler

KVK'nın 4.maddesinde kişisel verilerin işlenmesinde uyulması gereken genel ilkeler hükme bağlanmıştır. İşleme faaliyeti; kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi verilerin üzerinde gerçekleşen her türlü işlem olarak tanımlanmaktadır.
Söz konusu işleme faaliyetlerin KVK uyarınca ancak Kanunda ve diğer kanunlarda öngörülen usul ve esaslar çerçevesinde yapılması mümkündür. Bunun yanı sıra, KVK uyarınca Kişisel verilerin işlenmesinde aşağıda belirtilmiş olan ilkelere uyulması zorunludur:

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlar için işlenme.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenmesinde veri sorumlusunun veri işleme amacını açık ve kesin olarak belirlemesi ve söz konusu amacın meşru olması gerekmektedir. Belirtilen amaç dışında, başka bir amaçla veri işlenmesi halinde veri sorumluları bu fiillerinden dolayı sorumlu olacaklardır. Ayrıca amacın meşru olması, veri sorumlusunun işlediği verilerin yaptığı iş veya sunduğu hizmet ile bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.

Veri sorumlularının ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uymaları, yoksa verileri ancak işlendikleri amaç için gerekli olan süre kadar muhafaza etmeleri gerekmektedir. Saklanması için geçerli bir sebebin olmaması durumunda verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Gelecekte kullanma ihtimalinin olmasına dayanarak verilerin saklanması mümkün değildir. Anonim hale getirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade etmektedir. Bunların yanı sıra kişisel verinin sahibinin verilerinin silinmesini ya da yok edilmesini talep etmesi halinde rızasının olup olmadığına bakılmaksızın bu işlem gerçekleştirilmelidir.

Kişisel verilerin işlenmesi

01 Hukuka ve dürüstlük kurallarına uygun olma

02 Doğru ve gerektiğinde güncel olma

03 İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

04 Belirli, açık ve meşru amaçlar için işlenme

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

5. Kişisel verilerin işlenme şartları

Kişisel veriler, ilgili kişinin açık rızası veya KVK'nın 5.maddesinde sayılan istisnalar dışında işlenememektedir. Açık rıza KVK'nın 3. maddesinde belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza olarak tanımlanmıştır. 95/46 EC sayılı Avrupa Birliği Direktifine göre rıza ise 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 olarak belirtilmiştir.

KVK'nın 5. maddesi uyarınca;

- Kanunlarda açıkça öngörülmesi,
- 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,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

şartlarından birinin varlığı halinde, kişisel veriler ilgili kişinin açık rızası aranmaksızın işlenebilecektir.
Yukarıda sayılan şartlardan birinin varlığı halinde, kişisel verilerin işlenmesi hususunda ilgili kişinin açık rızasının alınması kuralı aranmayacağından bu haller açık rıza alınmasının istisnası olarak kabul edilecektir.

Kişisel verilerin işlenme şartları
Kural: Açık rıza
İstisnalar (Açık rıza aranmaksızın veri işleme):

1. Kanunlarda açıkça öngörülmesi.
2. Fiili imkansızlık.
3. Bir sözleşmenin taraflarına ait kişisel verilerin işlenmesi.
4. Veri sorumlusunun hukuki yükümlülüğü.
5. İlgili kişi tarafından alenileştirme.
6. Hakkın tesisi, kullanılması veya korunması.
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

6. Özel nitelikli kişisel verilerin işlenme şartları

KVK'nın 6. maddesine göre, kural olarak özel nitelikli kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Ancak, sağlık ve cinsel hayat dışındaki kişisel veriler, yeterli önlemlerin alınması şartı ile kanunda öngörülen hallerde ilgili kişinin açık rızası olmaksızın işlenebileceklerdir. Yeterli önlemlerin ne olduğu Kişisel Verileri Koruma Kurulu ("Kurul") tarafından belirlenecektir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetilmesi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

Yukarıda belirtilmiş olan istisna haller Kanun'da tahdidi olarak sayılmıştır, dolayısıyla bu sebeplerin dışındaki hallerde özel nitelikli kişisel verilerin işlenmesi mümkün olmayacaktır.

7. Kişisel verilerin aktarılması şartları

7.1. Üçüncü Kişilere Aktarılma

KVK'nın 8. maddesinde, kişisel verilerin yurt içindeki 3. kişilere aktarılması düzenlenmektedir. Kişisel veriler kural olarak ilgili kişinin açık rızası olmaksızın işlenemez, ancak aşağıda belirtilen istisnalardan birinin bulunması halinde ilgili kişinin açık rızası olmaksızın aktarılabileceklerdir.

- Kanunlarda açıkça öngörülmesi,
- 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,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Sağlık ve cinsel hayat dışındaki hassas kişisel veriler ise, yeterli önlemlerin alınması şartı ile kanunda öngörülen hallerde ilgili kişinin açık rızası olmaksızın aktarılabileceklerdir. Sağlık ve cinsel hayata ilişkin kişisel veriler de ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetilmesi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın aktarılabilir. Öte yandan, KVK'nın 8. maddesinde diğer kanunlarda yer alan kişisel verilerin aktarılmasına ilişkin hükümlerin saklı olduğu belirtilmiştir.

7.2. Yurt Dışına Aktarılma

KVK'nın 9. Maddesinde kişisel verilerin ve hassas nitelikli kişisel verilerin yurt dışına aktarılması düzenlenmiştir. Kural olarak kişisel veriler, ilgilinin açık rızası olmaksızın yurt dışına aktarılamaz. Ancak, yukarıda detaylı şekilde açıklanmış olan 3. kişilere açık rıza olmaksızın veri aktarımı yapılmasının istisna halleri burada da geçerli olacaktır.

Kişisel veriler aktarım yapılacak yabancı ülkede;

- Yeterli korumanın bulunması,
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabileceklerdir.

Kişisel verilerin aktarıldığı yabancı ülkelerde yeterli korumanın bulunup bulunmadığı Kurul tarafından belirlenerek ilan edilecektir. Öte yandan, KVK'nın 9. maddesinde diğer kanunlarda yer alan kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlerin saklı olduğu belirtilmiştir.

8. Veri sorumlusunun yükümlülükleri

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.

İlkelere uyum sağlama	İşleme şartlarına uyum sağlama	Aydınlatma yükümlülüğü
Silme/yok etme/ Anonimleştirme	Veri sorumluları siciline kaydolma	Aktarım yasağı/yurt dışına aktarım yasağı
İlgilinin başvurusuna yanıt verme	Teknik ve idari tedbirler alma	Denetim yapma

Veri sorumlusu KVK'da kişisel verilerin işleme amaçları ile vasıtalarını belirleyen ve veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. Veri işleyen ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak belirtilmiştir. Veri sorumlusu, kişisel verilerin kendi adına başkası tarafından işlenmesi halinde aşağıda belirtilecek olan yükümlülüklerin yerine getirilmesi hususunda bu kişilerle birlikte sorumlu olacaktır.

8.1. Genel İlkelere Uyum Sağlama

Veri sorumlusunun kişisel verilerin işlenmesi sırasında, yukarıda açıklanmış olan; "hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkelerine uyma yükümlülüğü söz konusudur.

Veri sorumluları ile veri işleyenler öğrenmiş oldukları kişisel verileri kanuna aykırı olarak başkasına açıklayamayacak ve işleme amacı dışında kullanamayacaktır. Bu yükümlülükleri görevden ayrılmalarından sonra da devam edecektir. Söz konusu yükümlülüğün amacı, kişisel verilerin yalnızca işlendikleri belirli amaçla bağlantılı ve sınırlı olarak kullanılmalarını sağlamak ve de hukuka aykırı hareket edilmesini engellemektir.

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgili kişiye ve Kurul'a bildirecektir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntem ile ilan edecektir.

8.2. İşleme Şartlarına Uyum Sağlama

Veri sorumlusunun kişisel veriler işlenirken, işleme faaliyetinin kanunda belirtilmiş olan işleme şartlarına uygun olmasını sağlama yükümlülüğü bulunmaktadır. Yukarıda da belirtildiği üzere, kişisel verilerin işlenmesinde kural olarak açık rıza aranmaktadır. Bazı istisna hallerin varlığı halinde söz konusu rıza olmaksızın veri işleme meşru olacaktır. Veri sorumlusunun bu noktada bu şartları sağlama yükümlülüğünden bahsedilebilecektir.

8.3. Silme/Yok Etme/Anonimleştirme

Veri sorumlusunun kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde re'sen ya da ilgili kişinin talebi üzerine silmesi, yok etmesi veya anonimleştirmesi zorunlu tutulmuştur.

8.4. Aydınlatma Yükümlülüğü

Veri sorumlusu veya yetkilendirdiği kişi, kişisel verilerin elde edilmesi sırasında ilgili kişilere;

- Veri sorumlusunun ve varsa temsilcisinin kimliğini,
- Kişisel verilerin hangi amaçla işleneceğini,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceğini,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- İlgili kişinin haklarını bildirmekle yükümlü kılınmıştır.

Aydınlatma yükümlülüğü ile veri sorumlusunun ilgili kişinin bilgisi olmaksızın kişisel verilerinin işlenmesinin önüne geçilmesi ve taraflar arasındaki anlaşmazlıkların doğmasının engellenmesi amaçlanmıştır.

8.5. Teknik ve İdari Tedbirleri Alma

Veri sorumlusu; 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 tedbiri almak zorundadır. Kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, söz konusu tedbirlerin alınması hususunda veri sorumlusu ile bu kişiler müştereken sorumlu olacaklardır. Söz konusu yükümlülük KVK'nın 12. maddesinde 'Veri Güvenliğine İlişkin Yükümlülükler' başlığının altında düzenlenmiş olup korunmak istenen değer, ilgili kişinin kişisel verilerinin güvenliğidir.

8.6. Denetim Yükümlülüğü

KVK'nın 12. maddesinin devamında veri sorumlusu, kendi kurum veya kuruluşunda Kanun'a uygun hareket edilmesini sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmakla yükümlü kılınmıştır.

8.7. Veri Sorumluları Siciline kayıt

Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Kişisel Verileri Koruma Kurulunun gözetiminde tutulan Veri Sorumluları Siciline ("Sicil") kaydolmak zorundadır. Ancak, kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma gibi hallerde Kurul tarafından bu zorunluluğa istisna getirilebilecektir. Söz konusu objektif kriterleri belirleme yetkisi Kurula aittir.

Sicile başvuruda; veri sorumlusu ve varsa temsilcisinin kimlik bilgileri, kişisel verilerin hangi amaçla işleneceği, veri konusu kişi grubu ve bu kişilere ait veri kategorileri hakkındaki açıklamalar, kişisel verilerin aktarılabileceği alıcılar, yabancı ülkelere aktarımı öngörülen kişisel veriler, kişisel veri güvenliğine ilişkin alınan tedbirler ve kişisel verilerin işlendikleri amaç için gerekli olan azami süre yer almalıdır.

8.8. İlgilinin başvurusunu yanıtlama yükümlülüğü

Kişisel verileri işlenen kişi, Kişisel Verilerin Korunması Kanununun uygulanmasıyla ilgili taleplerini veri sorumlusuna iletebilecektir. Veri sorumlusuna söz konusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç 30 gün içerisinde ücretsiz olarak sonuçlandırma yükümlülüğü getirilmiştir. Eğer bu işlem maliyet gerektiriyor ise Kurulun belirleyeceği tarifeye göre ücret alınabilecektir. Veri sorumlusu bu talebi kabul ya da reddedebilir. Reddetmesi halinde gerekçesini açıklaması gerekmektedir ve cevabı ilgili kişiye yazılı olarak veya elektronik ortamda bildirecektir. Talebin kabul edilmesi halinde veri sorumlusunun gereğini yerine getirmesi gerekmektedir.

9. İlgili kişinin hakları

Kanun uyarınca herkes kendisiyle ilgili aşağıda belirtilen hususlarda veri sorumlusuna başvurma hakkına sahiptir:

- Kişisel verilerinin işlenip işlenmediğini öğrenme,
- İşlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,
- İşlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerinin silinmesini veya yok edilmesini isteme,
- Kişisel verilerin aktarıldığı üçüncü kişilerin, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesinin ve işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerinin silinmesini veya yok edilmesinin talep edilebileceği hususlarında bildirilmelerini isteme,
- İşlenen verilerin yalnızca otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme.

10. Veri sorumlusuna başvuru ve şikâyet mekanizması

KVK'nın 13. maddesi uyarınca kişisel verileri işlenen ilgili kişi Kanun'un uygulanması ile ilgili taleplerini veri sorumlusuna iletebilecektir.

Talebi alan veri sorumlusu ise talepleri en geç 30 gün içinde ücretsiz olarak sonuçlandırmakla yükümlü kılınmıştır. Söz konusu işlem ayrıca bir maliyet gerektiriyorsa Kurul'un belirlemiş olduğu tarife ücreti alınabilecektir.

Veri sorumlusu 30 gün içerisinde yapacağı incelemenin ardından talebi kabul veya gerekçesini açıklayarak reddetmek zorundadır. Ayrıca cevabını ilgili kişiye bildirme yükümlülüğü getirilmiştir. Veri sorumlusunun talebi kabul etmesi halinde gereğini yerine getirmesi, hatalı ise alınan ücreti ilgiliye iade etmesi hükme bağlanmıştır. Bu durumda ilgili kişinin etmiş olduğu talebe konu hususta veri sorumlusunun hatalı olması düzenlenmiştir.

İlgili kişinin yukarıda açıklanmış olan 13. madde uyarınca yapmış olduğu başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya başvuruya süresinde cevap verilmemesi halinde ilgili kişiye, veri sorumlusunun cevabını öğrendiği tarihten itibaren 30 ve her halde 60 gün içerisinde Kurul'a şikâyette bulunma hakkı tanınmıştır. Ancak söz konusu şikâyet yoluna ancak veri sorumlusuna başvuru yolunun tüketilmesinin ardından başvurulması mümkün olacaktır. İlgilinin kişilik haklarının ihlal edilmesi halinde genel hükümlere göre tazminat talep edebilme hakkı KVK 14. uyarınca saklı tutulmuştur.

Kurul, ilgili kişinin yapacağı şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda

kendiliğinden, görev alanına giren konularda gerekli incelemeyi yapacaktır. Dolayısıyla ilgili kişinin şikâyeti üzerine Kurul'un yalnızca ilgili şikâyet konusuna ilişkin inceleme yapma hakkına sahip olduğu hükme bağlanmıştır.

Veri sorumluları, devlet sırrı niteliğindeki bilgi ve belgeler hariç, talep edilen bilgi ve belgeleri Kurul'a 15 gün içinde göndermek veya gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadırlar.

Kurul, talep üzerine şikâyeti inceleyerek ilgililere cevap verecektir, eğer şikâyet tarihinden itibaren 60 gün içerisinde cevap verilmez ise talep reddedilmiş sayılacaktır. Kurul'un vermiş olduğu cevabın şikâyeti kabul veya ret anlamı taşıyacak açıklıkta olmaması halinde, Kurul'un kararına karşı dava açılması mümkündür.

Yahut Kurul'un işlemini tamamlaması için KVK'da bu hususta bir hüküm bulunmadığı için, İdari Yargılama Usulü Kanunu (İYUK) uyarınca 6 ay beklenmesi mümkün olacaktır. 6 aylık bekleme süresi sona erdikten sonra Kurul aleyhine 60 gün içerisinde dava açılabilecektir.

Kurul, ihlalin varlığına karar vermesi halinde, tespit edilen hukuka aykırılıkların veri sorumluları tarafından giderilmesine karar vererek durumu ilgililere tebliğ edecektir. Kanuna aykırı bir uygulamanın varlığının tespiti halinde veri sorumlusuna hukuka aykırılığın düzeltilmesi için 30 gün süre verilecektir. Söz konusu süre kararın ilgililere tebliğinden itibaren başlayacak olup, hukuka aykırılığın giderilmemesi halinde KVK'nın aşağıda açıklanacak olan 18. maddesi uyarınca 25.000 ila 1.000.000 TL değerinde idari para cezası yaptırımı uygulanacaktır.

Kurul'a ayrıca telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verme yetkisi tanınmıştır. Kurul'a verilmiş olan bu yetkinin idare hukukundaki yürütmeyi durdurma kararı ile benzerlik gösterdiğini söylemek mümkündür.

11. Kişisel verilerin korunması kurumu ve kişisel verilerin korunması kurulu

Kişisel Verilerin Korunması Kurumu (''Kurum''), KVK'da verilen görevleri yerine getirmek üzere kurulmuş olan bir kamu tüzel kişiliğidir. KVK'nın 19. maddesinin gerekçesinde, Avrupa Konseyinin 108 sayılı Sözleşmesi'nin ve Avrupa Birliğinin 95/46/EC sayılı Direktifi 'nin, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere fonksiyonel olarak bağımsız bir şekilde görev yapacak otoritelerin oluşturulmasını öngördüğü belirtilmiştir. Ek olarak, Avrupa Birliği üyesi tüm ülkelerde veri koruma kurullarının görevlerinde bağımsız otoriteler şeklinde yapılandırıldığından bahsedilmiştir. KVK'nın 19. maddesinin 2. fıkrasında Kurum'un Başbakanlık ile olduğu hükme bağlanmıştır, bunun yanında Kurum'un idari ve mali özerkliğe sahip olacağı belirtilmiştir.
Kurum'un görevleri, KVK'nın 20. Maddesinde;

- Görev alanındaki uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak ve yaptırmak,
- İhtiyaç duyulması halinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle işbirliği yapmak,
- Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak,
- Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Hakları İnceleme Komisyonuna ve Başbakanlığa sunmak,
- Kanunlarla verilen diğer görevleri yerine getirmek olarak belirtilmiştir.

Kurum'un yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Hakları İnceleme Komisyonuna ve Başbakanlığa sunması, şeffaflığının ve hesap verilebilirliğinin sağlanması için getirilmiş bir görevdir.

Kişisel Verilerin Korunması Kurulu'nun ("Kurul"), KVK'nın 19. Maddesinde Kurum'un karar organı olduğu hükme bağlanmıştır. Yine, Avrupa Konseyinin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifine uygun şekilde bağımsız bir organ olduğu belirtilmiştir. Kurul'un, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getireceği ve kullanacağı, görev alanına giren konularla ilgili olarak hiçbir organ veya kişinin Kurul'a emir vermeyeceği hüküm altına alınmıştır.

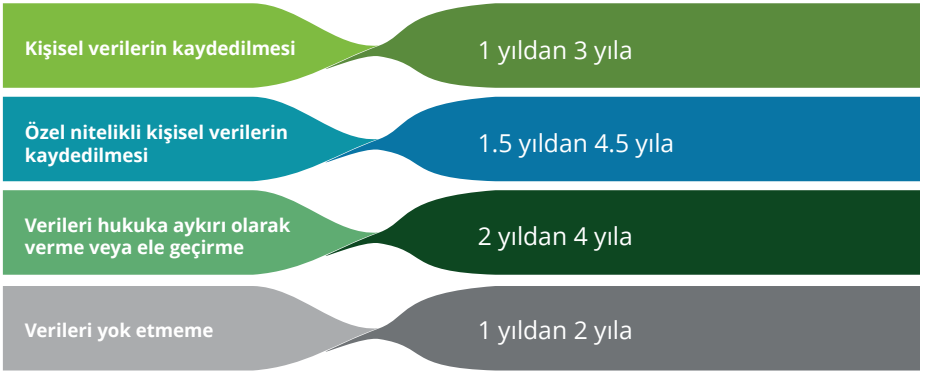
Kurul'un görevleri, KVK'nın 22. maddesinde;

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,
- Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak,
- Şikâyet üzerine veya kendiliğinden ihlal iddiasını öğrenmesi durumunda görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak,
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek,
- Veri Sorumluları Sicili'nin tutulmasını sağlamak,
- Kurul'un görev alanı ile Kurum'un işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak,
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak,
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak,
- KVK'da öngörülen idari yaptırımlara karar vermek,
- Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek,
- Kurum'un; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek ve Kurum'un stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak,
- Kurum'un performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak,
- Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak,
- Kanunlarla verilen diğer görevleri yerine getirmek olarak belirtilmiştir.

12. Yaptırımlar

12.1 Suçlar

KVK'nın "Suçlar" başlıklı 17. maddesi uyarınca TCK'nın 135 ila 140.'ıncı maddelerine atıfta bulunulmuştur. Bu maddelere göre suç teşkil eden fiiller ve cezaları aşağıdaki şekilde öngörülmüştür:



135): Hukuka aykırı olarak kişisel verileri kaydetme suçunun işlenmesi halinde 1 ila 3 yıl arasında hapis cezası verilir. Kişisel verinin siyasi, felsefi veya dini görüş, ırki köken, ahlaki eğilim, cinsel yaşam, sağlık durumu veya sendikal bağlantıya (özel nitelikli kişisel veri) ilişkin olması halinde 1,5 yıl ila 4,5 yıla kadar olacak şekilde yarı oranında artırılır.

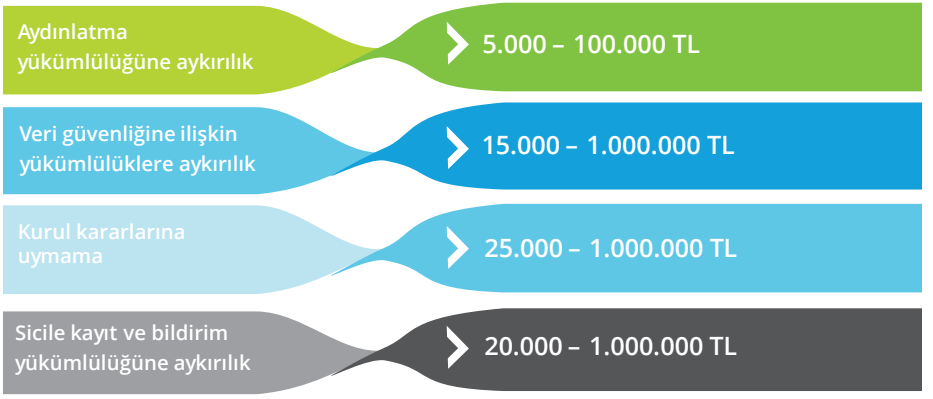
- **Verileri hukuka aykırı olarak verme veya ele geçirme (TCK 136):** Kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme suçunun işlenmesi halinde 2 ila 4 yıl arasında hapis cezası verilir.
- **Verileri yok etmeme (TCK 138):** Kanunların belirlediği sürelerin geçmiş olmasına karşın, verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmemeleri halinde 1 ila 2 yıl arasında hapis cezası verilir. Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek ceza bir kat artırılacaktır.
- **Tüzel kişiler hakkında güvenlik tedbiri uygulanması (TCK 140) :** Yukarıdaki suçların işlenmesi dolayısıyla tüzel kişiler hakkında onlara özgü güvenlik tedbirlerine hükmolacağı belirtilmiştir.

12.2. Kabahatler

KVK'nın " Kabahatler" başlıklı 18. maddesi uyarınca aşağıdaki yaptırımlar öngörülmüştür:

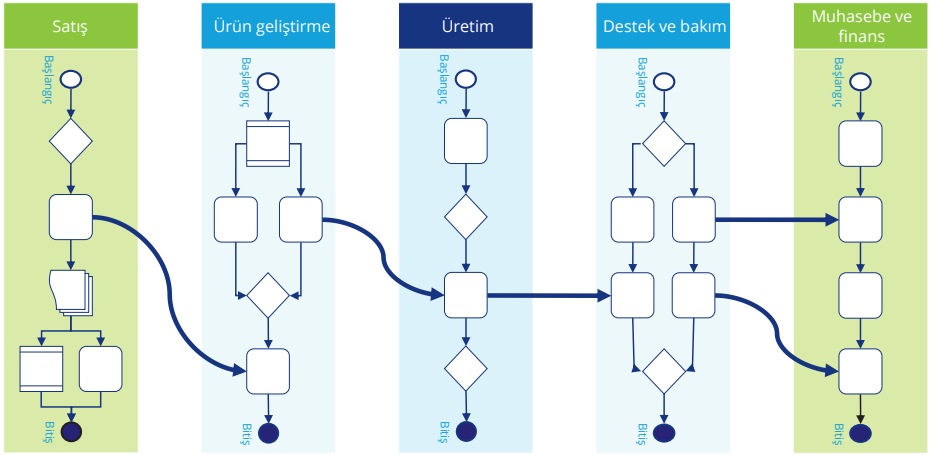
- Aydınlatma yükümlülüğüne aykırılık halinde 5.000 ila 100.000 TL,
- Veri güvenliğine ilişkin yükümlülüklere aykırılık halinde 15.000 ila 1.000.000 TL,
- Kurul tarafından verilen kararları yerine getirmeme halinde 25.000 ila 1.000.000 TL,
- Sicile kayıt ve bildirim yükümlülüğüne aykırı hareket etme halinde 20.000 ila 1.000.000 TL idari para cezası.

Bunun yanı sıra idari yaptırımlara Kurul tarafından karar verileceği hükme bağlanmış olup madde gerekçesinde idari para cezalarının alt ve üst sınırlarının kanun koyucu tarafından bilinçli olarak geniş tutulduğu belirtilmiştir. Kurul, idari yaptırımlara karar verirken kabahatin haksızlık seviyesini, failin kusurunu ve ekonomik durumunu dikkate alacaktır. Dolayısıyla Kurul'un yetkisinin çok geniş olduğu görülmektedir, miktarları çok yüksek olan idari para cezalarına hükmedilmesinin önlenebilmesi açısından veri sorumlularının söz konusu yükümlülükleri yerine getirmesi büyük derecede önem taşımaktadır.



KVK'nın 18. madde gerekçesinde, yukarıda belirtilmiş olan idari yaptırımların veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişilerine uygulanacağı belirtilmiştir.

13.Mahremiyet Etki Analizi ve Alınması Gereken Aksiyonlar



Kişisel Veri Yaşam Döngüsü

Veri akış diyagramları bizlere verilerin şirketlere hangi noktalardan nasıl girdiğini ve daha sonra hangi yollarla aktarıldığını veya imha edildiğini görsel olarak ifade etmede yardımcı olur. Böyle bir çalışma ile kişisel verilerin şirketler için uygun görülen yaşam döngüsü de çizilmiş olur ve bu akışın dışındaki kişisel veri hareketleri veri koruma ihlali olarak adlandırılabilir.

Verinin Toplanması

Kişisel veriler birçok farklı kanaldan elektronik veya fiziksel yöntemlerle toplanabilir. Hukuksal olarak bu noktalarda gerekli rızaların alınması ve bu rızaların muhafaza edilebilmesi için süreçler tesis edilmelidir. Özellikle elektronik olarak alınan rızaların kanıtlanabiliyor olması gerekmektedir. Bunun için zaman damgası kullanmak en yaygın ve kabul gören yöntemdir. Elektronik veri toplama noktalarında bilişim güvenlik uzmanlarının görüşlerini almak siber tehdit ara yüzlerinin kontrollü olarak hizmet vermesine yardımcı olur. Konu uzmanlarının yönlendirmeleri ile sıkılaştırılmış veri giriş noktaları düzenli olarak denetimlere ve değerlendirmelere tabi tutulmaya devam etmelidir. Unutulmamalıdır ki bilgi güvenliği tek seferlik bir iş değildir.

Kişisel bilgiler, finans veriler ve fikri mülkiyet gibi hassas bilgiler organizasyon boyunca yatay hareket eder.

Kişisel Veri Envanteri

Veri sorumlusu hem kendi bünyesinde barındırdığı veriler, hem de üçüncü taraflara aktardığı veriler için bu kurallara uyulduğundan emin olmalıdır. Veri sorumlusu, veri işleyene, kendisi için kişisel verilerin kabul edilebilir kullanım kurallarını bildirmelidir.

Verinin Kullanılması

Kişisel verilerin kabul edilebilir kullanım kurallarının veri sorumlusu tarafından belirleniyor olması beklenir. Bu kurallar belirlenirken geçerli ve uygulanabilir kanunlar, düzenlemeler ve sözleşmelerden doğan yükümlülükler göz önünde bulundurulur. Sektörel olarak kabul görmüş ve öne çıkan iyi uygulamaları da değerlendirip şirket için uygulanabilir olanları hayata geçirmek, veri güvenliğinden doğabilecek riskleri yönetmekte faydalı olacaktır. Kullanım kuralları asgari olarak aşağıdaki başlıklarda tanımlanabilir:

- Erişim kontrolü
- Kullanıcı doğrulaması
- Erişim kaydı (log)
- Fiziksel güvenlik

Verinin Aktarımı

Fiziksel veya elektronik veri aktarımı için güvenli yöntemler belirlenmelidir. Elektronik ortamlarda veri aktarımı yapılırken mahremiyetinin korunması için kriptolu iletişim tercih edilir.

Verinin Saklanması

Yasal veya sözleşmelerden doğan kişisel veri saklama yükümlülükleri ortaya çıkartıldıktan sonra bu yükümlülüklerin nasıl yerine getirileceğine karar verilmelidir.

Verinin İmhası

Fiziksel veya elektronik ortamda bulunan kişisel verilerin imha edilmesi için uygun yöntemler şirketler tarafından belirlenip ilgililerin bu yöntemlere hakim olduğundan emin olunmalıdır. Basılı dokümanlar için en yaygın olarak kullanılan yöntem kağıt kıyma makinası kullanımıdır. Sabit disklerde veya taşınabilir belleklerde tutulan cihazlardaki verilerin imhası için farklı birçok yöntem bulunmaktadır. ABD Savunma Bakanlığı tarafından önerilen yöntem olan DoD 5220.22-M standardı ve Kanada İletişim Güvenlik Kurumu tarafından yayımlanan CSEC ITSG-06 standardı iyi uygulamalar arasında yer alır.

Mahremiyet Etki Analizi

Veri mahremiyeti konusundaki riskleri ortaya çıkartmada kullanılan en bilinen yöntem Mahremiyet Etki Analizi'dir. Sonucunda kişisel verilerin üzerindeki güvenlik ve uyum riskleri ortaya çıkartılır. Bu analiz mevcut ürün ve hizmetlere yapılabildiği gibi henüz hayata geçirilmemiş, tasarım aşamasındaki ürün ve hizmetlere de yapılabilir. Mevcut ürün ve hizmetler için yılda en az bir defa ve uyum ihtiyaçlarında, teknik altyapıda veya süreçlerde herhangi bir değişiklik olduğu zaman yapılması tavsiye edilir.
Analiz sonucunda çıkan risklerin yönetimi için klasik risk yönetimi teknikleri kullanılır. Analiz sonuçlarını değerlendirmedeki kritik başarı faktörlerinden birisi değerlendirme yapacak kişilerin riskler konusunda farkındalığının üst seviyede olması ve şirkette yetki sahibi olmalarıdır.

Denetim

Kişisel verilerin korunmasına ilişkin yapılabilecek denetimleri iki aşamalı olarak gerçekleştirebiliriz. İlk aşamada tasarım denetimi yapılır. Bu aşamada organizasyonların kişisel veri koruma politika ve prosedürlerinin yeterliliği değerlendirilir. İkinci aşamada ise uygulama denetimi yapılır. Mevcut politika ve prosedürlere ne kadar uyulduğu bu aşamada denetlenir. Bu tarz denetimlerdeki muhtemel kontrol alanları aşağıdaki gibi sıralanabilir:

- Organizasyon
- Aydınlatma, bildirim ve kayıt
- Kişisel veriye bireysel erişim
- Seçim ve rıza
- Güvenlik
- Bilgi yönetimi
- Veri aktarımı
- Olay müdahale
- Üçüncü tarafların yönetimi
- İzleme

Bilgi güvenliğinin temel prensipleri olan gizlilik, bütünlük ve erişilebilirlik ihtiyaçlarının ortaya çıkartılmış ve tespit edilen ihtiyaçların yerine getirilmesi için önlemlerin alınmış olması beklenir. Teknik altyapı üzerinde zafiyet oluşturabilecek eksikliklerin tespit edilip kapatılması için süreçlerin tasarlanmış ve uygulanıyor olması gerekir. Kişisel verilerin kabul edilebilir akışlarının şirketler tarafından belirlenmiş ve buna uygun olmayan kullanımları tespit edebiliyor olması gerekir.

Şirket dışına aktarımlarda izlenecek güvenli yöntemlerin dışına çıkılmıyor olması gerekir. Veri sorumlusu durumunda olduğumuz ve üçüncü taraflara aktardığımız verilerin istenen güvenlik ve mahremiyet düzeyinde tutulduğundan emin olmak için bir takım izleme ve denetleme süreçlerinin tanımlanmış olması gerekir. Bu süreçler ve ilgili raporlama ihtiyaçları şirketlerin uyum ekiplerine raporlanabilir.

Lerzan Nalbantoğlu
Ortak
lnalbantoglu@dlhukuk.com

Tel: (0212) 708 41 11
Cep: 0533 298 61 44

Asilhan Özkaya
Kıdemli Avukat
aozkaya@dlhukuk.com

DL Avukatlık Bürosu

Maslakno1 Plaza
Eski Büyükdere Caddesi
Maslak Mahallesi No:1 K18
Maslak 34398
Sarıyer, İstanbul

T: +90 (212) 708 41 10
F: +90 (212) 708 41 41

www.dlhukuk.com

© 2016. Daha fazla bilgi için DL Avukatlık Bürosu.