BELEDİYELER İÇİN KİŞİSEL VERİLERİN KORUNMASI

6698 Sayılı Kişisel Verilerin Korunması Kanunu

17 ŞUBAT 2020

Akdeniz Belediyeler Birliği

AKDENİZ BELEDİYELER BİRLİĞİ

İçindekiler

GİRİŞ

1978 yılında Antalya-Isparta ve Burdur Belediyelerinin ortaklığında kurulan, Akdeniz Belediyeler Birliği, 2005 yılında yürürlüğe giren Mahalli İdare Birlikleri Yasasına göre yeniden yapılandıktan sonra, bu çerçevede, tüm yönetim organları, teşkilat yapısı, yeni yasaya göre oluşturularak, Kurumsal yapısı tamamlanmıştır.

Bu organizasyon yapısı içinde görevlerini sürdüren Birliğimiz, Muğla, Denizli, Afyon, Malatya, Amasya, Çorum, Konya ve Mersin ili belediyelerinin üye olarak katılımları ile üye belediye sayısı 75'e ulaşmıştır.

Özellikle son yıllarda, bölge belediyeciliğinin gelişimine yönelik çalışmaları, üyeleri ile yakın işbirliği içinde üretilen programları ile alanında etkin bir kurum haline gelmiş, bu çerçevede hizmetlerini sürdürmektedir.

Üyesi olan belediyelerin, merkezi idare ile aralarındaki hizmet ve kaynak bölüşümü, mevzuat düzenlemesi konularında hak ve çıkarlarının savunulması, belediyeler arası koordinasyon sağlanması, bilgi ve deneyimlerin birbirine aktarılmasına aracılık edilmesi, üye belediyelerin ulusal ve uluslararası platformlarda temsil edilmesi, belediye hizmetlerinin ve beldelerin tanıtımına öncülük ve ortaklık edilmesi, birden fazla belediyenin ortak oluşturacağı projeleri ile bölge ve havza bazında geliştirecekleri projelerin hazırlanmasına ve hayata geçirilmesine ortaklık edilmesi, belediyelerde insan kaynaklarının geliştirilmesine yönelik hizmet içi eğitim programları uygulanması, ülkemizin AB üyeliği sürecine belediyelerimizin uyumu kapsamında ortak çalışmalar yürütülmesi, Türk mevzuatının, belediyelere tanıdığı hak ve yetkiler çerçevesinde yerel nitelikli hizmetler üretilmesi, alanlarında faaliyetlerimiz sürdürülmektedir.

Akdeniz Belediyeler Birliği olarak son zamanlarda oldukça popüler olmasıyla bilinen aslında bireylerin temel hak ve hürriyetlerinin kaçınılmaz bir objesi olan kişisel verilerin korunması, 6698 sayılı Kişisel Verilerin Korunması Kanunu, bilgi güvenliği tedbirleri ve benzeri konular gündemimiz olmuştur. Buna istinaden 24 Ocak 2020 tarihinde birliğimiz bünyesinde eğitim düzenlemiş olup iş bu raporla birlikte eğitim notlarımızı paylaşmaktayız.

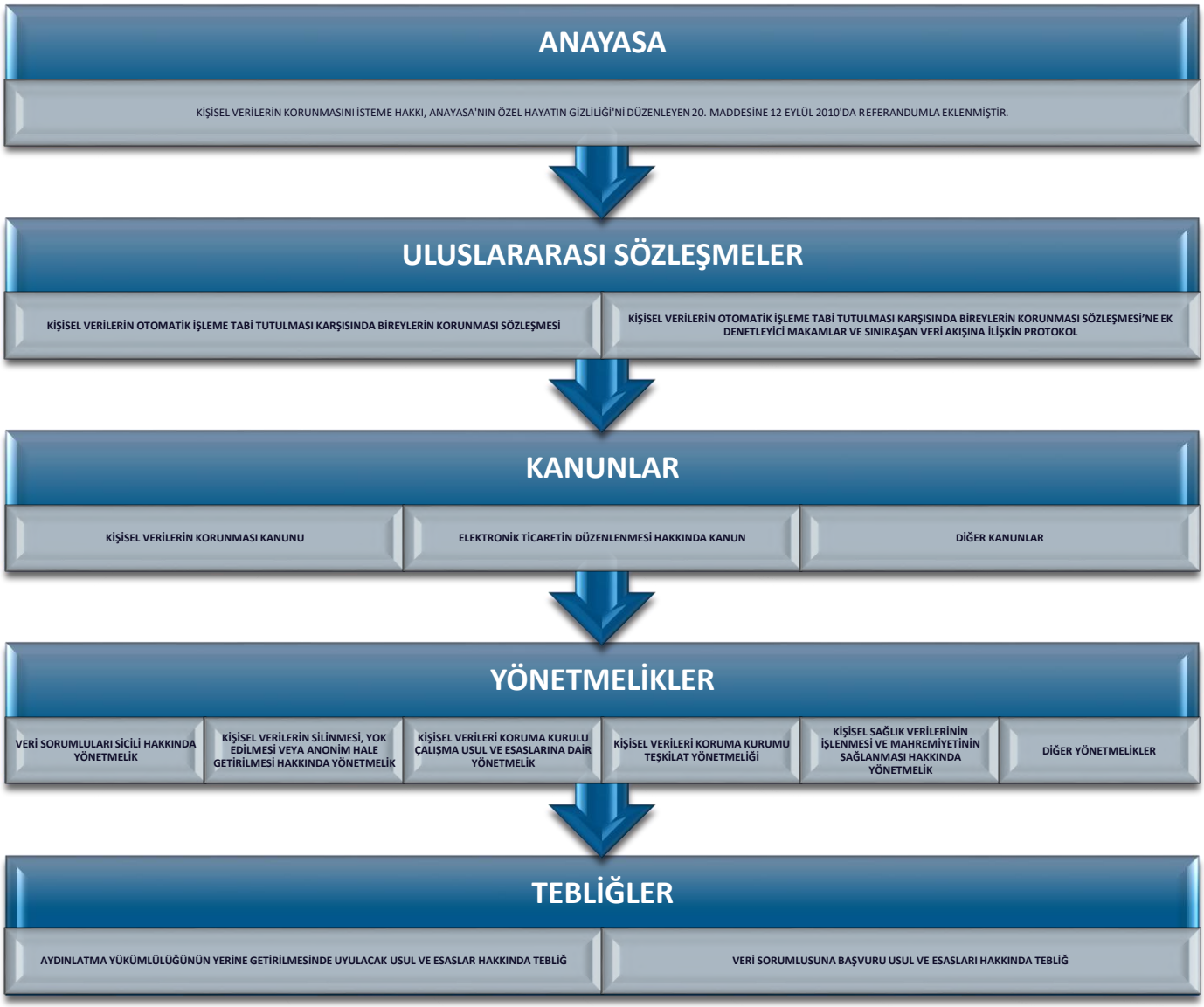
Bu raporda öncelikle belediyelerimizde kişisel verilerin korunması ve veri yönetimine dayanak teşkil eden 6698 sayılı Kişisel Verilerin Korunması Kanunu, bu

kanuna bağlı yönetmelikle ve ilgili kanun maddeleri ile kanuna göre yükümlülüklerini yerine getirmeyenlere uygulanacak idari para cezaları ve TCK kapsamındaki cezalar anlatılmıştır. Kanuna uyum sürecinde belediyeler açısından yapılması gerekenler sayılmıştır. E-Belediye sistemine geçiş sürecinde olan veya süreci tamamlayan belediyeler için kişisel verilerin korunması anlamındaki sorumlulukları ifade edilmeye çalışılmıştır. Bu rapor, ilgili kanuni düzenlemeler çerçevesinde üye belediyelerimizin veri yönetiminde ne şekilde hareket edeceklerine dair bir rehber niteliğinde hazırlanmıştır.

Bu raporda ve eğitimimizde emeği geçen **KoçArslan Hukuk & Danışmanlık** kurucuları **Av. Yusuf Enes ARSLAN** ve **Av. Mert KOÇ** ile birlikte **Siber Güvenlik Uzmanı Fatih Mehmet Dişçioğlu**'na ve tüm katılımcılarımıza teşekkür eder, raporun üye belediyelerimiz için faydalı olmasını dileriz.

AKDENİZ BELEDİYELER BİRLİĞİ

MEVZUAT


ANAYASA
KİŞİSEL VERİLERİN KORUNMASINI İSTEME HAKKI, ANAYASA'NIN ÖZEL HAYATIN GİZLİLİĞİ'Nİ DÜZENLEYEN 20. MADDESİNE 12 EYLÜL 2010'DA REFERANDUMLA EKLENMİŞTİR.
ULUSLARARASI SÖZLEŞMELER
KİŞİSEL VERİLERİN OTOMATİK İŞLEME TABİ TUTULMASI KARŞISINDA BİREYLERİN KORUNMASI SÖZLEŞMESİ
KİŞİSEL VERİLERİN OTOMATİK İŞLEME TABİ TUTULMASI KARŞISINDA BİREYLERİN KORUNMASI SÖZLEŞMESİ'NE EK DENETLEYİCİ MAKAMLAR VE SINIRAŞAN VERİ AKIŞINA İLİŞKİN PROTOKOL
KANUNLAR
KİŞİSEL VERİLERİN KORUNMASI KANUNU
ELEKTRONİK TİCARETİN DÜZENLENMESİ HAKKINDA KANUN
DİĞER KANUNLAR
YÖNETMELİKLER
VERİ SORUMLULARI SİCİLİ HAKKINDA YÖNETMELİK
KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ HAKKINDA YÖNETMELİK
KİŞİSEL VERİLERİ KORUMA KURULU ÇALIŞMA USUL VE ESASLARINA DAİR YÖNETMELİK
KİŞİSEL VERİLERİ KORUMA KURUMU TEŞKİLAT YÖNETMELİĞİ
KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİ VE MAHREMİYETİNİN SAĞLANMASI HAKKINDA YÖNETMELİK
DİĞER YÖNETMELİKLER
TEBLİĞLER
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ
VERİ SORUMLUSUNA BAŞVURU USUL VE ESASLARI HAKKINDA TEBLİĞ

KİŞİSEL VERİLERİN KORUNMASI KANUNU (KVKK)

24/03/2016 tarih ve 6698 sayılı kanun ile hem kamunun hem de özel sektörün kişisel verileri ne şekilde işleyebileceğinin esasları düzenlenmiştir.

Kişisel verilerin; elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması veya sınıflandırılması gibi her türlü işlem kişisel veri işleme olarak kabul edilmektedir ve Kanun'da düzenlenen kurallara uygun olmalıdır.

Kişisel Verilerin Korunmasına Neden İhtiyaç Duyulmuştur?

Gerek kamu, gerekse özel kurum ve kuruluşlar, bir görevin yerine getirilmesi veya bir hizmetin sunumuyla bağlantılı olarak, kişis**el veri niteliğindeki bilgileri** uzun süredir toplamaktadırlar. Bu durum, bazen kanunlardan kaynaklanmakta bazen kişilerin rızasına veya bir sözleşmeye dayanmakta bazen de yapılan işlemin niteliğine bağlı olarak ortaya çıkmaktadır. Belirtmek gerekir ki, kişilerin temel hak ve hürriyetlerinin veri işleme sürecinde de korunmas**ı öncelikli konulardan biridir.**

Ayrıca, sosyal ve ekonomik hayatın düzen içinde sürdürülmesi, kamu hizmetlerinin etkin biçimde sunumu, mal ve hizmetlerin ekonominin gereklerine uygun biçimde geliştirilmesi, dağıtımı ve pazarla**nması için kişisel** verilerin toplanması kaçınılmaz olmakla birlikte, kişisel verilerin sınırsız ve gelişigüzel toplanmasının, yetkisiz kişilerin erişimine açılmasının, ifşası, amaç dışı ya da kötüye kullanımı sonucu kişisel hakların ihlal edilmesinin önüne geçilmesi gereklidir.

Bunun yanı sıra, Avrupa Konseyi tarafından, tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme", 28 Ocak 1981 tarihinde imzaya açılmış ve ülkemiz tarafından da imzalanmıştır. Bu sözleşme 17 Mart 2016 tarih ve 29656 sayılı Resmî Gazetede yayımlanarak iç hukuka dâhil edilmiştir. 108 sayılı Sözleşmenin 4. maddesi çerçevesinde, iç hukukta kişisel verilerin korunmasına yönelik yasal düzenleme yapılması gerekli hale gelmiştir.

Nitekim Anayasa Mahkemesinin 9 Nisan 2014 tarih ve E:2013/122, K:2014/74 sayılı kararında da; "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak,

bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı […]" amaçladığı tespit edilerek, "kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler" sebebiyle kişisel verilerin geçmişte olduğundan çok daha fazla korunmaya **muhtaç olduğu ifade edilmiştir.**

Kişisel Verilerin Korunması Kanunu Kimleri Kapsamaktadır?

Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin (kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi) parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

Bu doğrultuda, özel sektörde faaliyet gösteren kuruluşlar ile kamu kurum ve kuruluşları bakımından bir ayrım yapılmamış olup, öngörülen usul ve esasların tüm kurum ve kuruluşlar açısından uygulanması benimsenmiştir. Kanunda verisi işlenen gerçek kişilerden bahsedildiği için hak ehliyetine sahip olan herkes Kanun kapsamındadır.

Bu bağlamda belediyeler de işledikleri kişisel veriler yönüyle Kanun kapsamındadır.

Kanunda "kişisel verileri işlenen gerçek kişiler" ifadesi kullanıldığından, kişisel verileri işlenen tüzel kişiler bu Kanunun kapsamı dışında tutulmuştur.

Veri işleme faaliyetini gerçekleştirenler açısından ise Kanunda gerçek kişi tüzel kişi ayrımına gidilmemiştir. Ancak, veri kayıt sisteminin parçası olmaksızın veri işleyenler Kanunun kapsamı dışında tutulmuştur

Kanunun 28. maddesinde, bazı hallerde Kanun hükümlerinin uygulanmayacağı belirtilmektedir. Bu çerçevede, Kanun kapsamına girmeyen haller, 28. maddede tamamen veya kısmen kapsam dışı olan haller olmak üzere ikili bir ayrıma tabi tutulmuştur. Bu maddenin 1. fıkrasında tam istisnalar, 2. fıkrasında ise kısmi istisnalar düzenlenmiştir. Tam istisna halinde Kanun hükümleri hiçbir şekilde uygulanmamakta iken, kısmi istisna hallerinde, Kanunun sadece bazı hükümleri (aydınlatma yükümlülüğü, ilgili kişinin hakları ve veri sorumluları siciline kayıt) uygulanmamaktadır.

KAVRAMLAR

Kişisel verilerin korunması, kişisel verilerin işlenmesinin disiplin altına alınması ile temel hak ve özgürlüklerin korunmasıdır.

Kişisel verilerin korunması, temelde verilerin değil, bu verilerin ilişkili olduğu kişilerin korunmasını amaçlamaktadır. Başka bir ifade ile verilerin korunması; kişileri, onlar hakkındaki verilerin tamamen veya kısmen otomatik olan ya da otomatik olmayan yollarla işlenmesinden doğacak zararlardan koruma amacına yönelmiş ve kişisel verilerin korunmasına ilişkin ilkelerde somutlaşmış idari, teknik ve hukuki önlemleri ifade eder. Bu anlamda kişisel verilerin korunmasının, kişilere ilişkin verilerin toplanması, saklanması, kullanılması ve aktarılması gibi veri işleme süreçlerinin bütün aşamalarını kapsar şekilde bireylere kontrol hakkını yeniden kazandırmayı amaçladığı söylenebilir. Bu amaç kapsamında kişisel verilerin korunması, kişinin verilerinin geleceğini bizzat kendisinin belirleme hakkını ifade eder. Aynı zamanda bu koruma insan onurunun ve kişilik hakkının da bir gereğidir.

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir. Buna göre;

1. Gerçek kişiye ilişkin olma: Kişisel veri, gerçek kişiye ilişkin olup, tüzel kişilere ilişkin veriler kişisel verinin tanımının dışındadır. Dolayısıyla, bir şirketin ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin bilgiler (bir gerçek kişiyle ilişkilendirilebilecekleri durumlar haricinde) kişisel veri sayılmayacaktır.
2. Kişiyi belirli veya belirlenebilir kılması: Kişisel veri, ilgili kişinin doğrudan kimliğini gösterebileceği gibi, o kişinin kimliğini doğrudan göstermemekle birlikte, herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm bilgileri de kapsar.
3. Her türlü bilgi: Bu ifade son derece geniş olup, bir gerçek kişinin; adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.

Kanunda hangi bilgilerin kişisel veri olarak kabul edileceğine ilişkin sınırlı sayım yoluna gidilmediğinden, kapsamının genişletilmesi mümkündür. Önemli olan verinin kişi ile ilişkilendiriliyor olması ya da onu tanımlayabilmesidir.

Örneğin, takma isimler tek başına veya başka kaynaklarla birleştirildiğinde kişiyi tanımlamayı sağlayabilecek nitelikte ise bu tarz veriler de kişisel veri olarak kabul edilir. Ayrıca, sıkça kullanılan kimliği belirli veya belirlenebilir gerçek kişiyle ilişkili müşteri şikayet raporları, çalışan performans değerlendirme raporları, mülakat değerlendirme raporları gibi raporlar, ses veya görüntü kayıtları, resimler, kullanıcı işlem kayıtları gibi kayıtlar, özgeçmiş, bordro, fatura, banka dekontları, kredi kartı ekstreleri, nüfus cüzdanı fotokopileri gibi belgeler ve mektup, davet yazıları gibi yazılar/kayıtlar içinde yer alan veriler de kişisel veri olarak addedilebilir.

Ancak yine de bunların kişisel veri olup olmadığı her somut olayın özelliğine göre "kişiyi tanımlayabilme" kabiliyeti dikkate alınarak değerlendirilmelidir.

Özel nitelikli kişisel veriler, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikteki verilerdir. Kanunda, hangi kişisel verilerin özel nitelikli kişisel veri olduğu tek tek belirtilmiş olup, bu sayılanlar dışındakiler özel nitelikli kişisel veri olarak kabul edilemez. Bu bakımdan, özel nitelikli kişisel verilerin sınırlı olarak sayıldığı kabul edilir.

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 verilerdir.

Buna göre, hassas veriler kişisel verilerin daha fazla koruma uygulanan küçük bir grubu olarak değerlendirilebilir.

İlgili kişi, kişisel verisi işlenen gerçek kişiyi ifade eder. Kanunda, yalnızca gerçek kişilerin verilerinin korunması öngörülmüş, tüzel kişilerin verileri Kanun kapsamı dışında tutulmuştur.

Kanunda yer alan kişisel verinin tanımı gereği, tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde, bu veriler de Kanun kapsamında koruma altındadır.

Ancak, burada korunan menfaat tüzel kişiye değil, düzenlemenin temellendirdiği öncelik gereği belirlenen ya da belirlenebilecek gerçek kişiye ait olacaktır. Çünkü Kanun, tüzel kişilere ait verilerin korunmasını hiçbir şekilde düzenlememektedir.

Kişisel verilerin işlenmesi, 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 işlemi ifade eder.

Örneğin, kişisel verilerin sadece bir hard diskte, CD'de, sunucuda depolanması, anılan verilerle başkaca hiçbir işlem yapılmasa da bir veri işleme faaliyetidir.

Dolayısıyla veri işleme kapsamına giren eylemler sınırlı sayıda olmayıp, kişisel verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir.

Açık rıza, belirli bir konuya ilişkin, bilgilendirilmeye dayanan özgür irade açıklamasıdır.
Açık rızanın üç unsuru bulunmaktadır:

1. Belirli bir konuya ilişkin olması: Veri işlemek üzere verilen rızanın geçerli olması için rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması gerekir. Buna göre genel bir irade açıklaması ile "kişisel verilerimin işlenmesini kabul ediyorum" şeklinde açık uçlu ve belir-siz bir rıza tek başına Kanun bağlamında açık rıza olarak kabul edilemez. Diğer bir ifade ile battaniye rızalar hukuken geçersizdir.

2. Rızanın bilgilendirmeye dayanması: Açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza gösterebilmesi için neye rıza gösterdiğini bilmesi gerekir. Bu

kapsamda, kişiye yapılacak bilgilendirme, mutlaka verinin işlenmesinden önce yapılmalı ve veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmelidir.
Bilgilendirme yapılırken elde edilecek kişisel verilerin hangi amaçlarla kullanılacağı açıkça belirtilmeli, kişinin anlamayacağı terimler ya da yazılı bilgilendirme yapıldığında okumakta güçlük çekeceği oranda küçük puntolar kullanılmamalıdır.

3. Özgür iradeyle açıklanması: Kişinin irade beyanı olan rıza, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacaktır. Cebir, tehdit, hata ve hile gibi iradeyi sakatlayan hallerde kişinin özgür biçimde karar vermesi mümkün değildir.
Örneğin, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göster-memenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez.

Açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir.

Örneğin, bir hizmetten yararlanılmasının üyelik şartına bağlandığı yerlerde, üye olmak isteyen ilgili kişinin parmak izinin alınması ve işlenmesinin üyelik sözleşmesinin kurulması için zorunluluk olarak öngörülmesi hukuka aykırı olacaktır. Çünkü bu şekilde alınan açık rıza özgür irade ile açık rıza verilmesi ilkesine ve ölçülülük ilkesine aykırı olacaktır.

Açık rıza beyanı herhangi bir şekil şartına tabi değildir. Önemli olan açık rızanın Kanundaki unsurları taşıması ve ispatlanabilir olmasıdır. Dolayısı ile sözlü, yazılı, elektronik ortam vb. yöntemlerle açık rıza alınması mümkündür. Bununla birlikte, açık rızanın yazılı olduğu durumlarda, açık rıza metinleri açık, anlaşılır ve yalın bir şekilde kaleme alınmalıdır. Ayrıca, açık rızanın, olumlu bir irade beyanı içermesi gerekmektedir. Diğer bir ifade ile açık rızanın şüpheye yer vermemesi gerekmekte, rızanın talep edilmesine ve alınmasına ilişkin işlemler, ilgili kişinin bu konudaki niyetini açık bir şekilde ortaya koyar nitelikte olmalıdır. Açık rızanın alındığı konusundaki ispat yükü ise veri sorumlusuna aittir.

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Bu kişiler, gerçek kişiler olabileceği gibi, kamu kurumları, şirketler,

dernekler veya vakıflar gibi tüzel kişiler de olabilecektir. Veri sorumlusu, işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek kişidir.

Veri sorumlusunun tespiti için kişisel verilerin işlenmesi ve işlenme amacı, işlenecek kişisel veri türleri, işlenen kişisel verilerin hangi amaçlarla kullanılacağı, hangi kişilerin kişisel verilerinin işleneceği, kişisel verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kimlerle paylaşılacağı, ne kadar süreyle saklanacağı, ilgili kişilerin erişim hakkı ve diğer haklarının uygulanıp uygulanmayacağı gibi hususlara kimin karar verdiği dikkate alınır.

Burada belirtilmesi gereken diğer bir husus ise, eğer veri işleme faaliyeti bir tüzel kişilik tarafından gerçekleştiriliyorsa, burada veri sorumlusu tüzel kişinin kendisidir. Tüzel kişiliğin içerisinde veri işleme faaliyetlerinden sorumlu olan gerçek kişiler Kanunun uygulanması bakımından veri sorumlusu sayılmazlar. Veri sorumlusunun tüzel kişi olması halinde, veri sorumlusu yükümlülüğü ilgili tüzel kişilik üzerinde doğacaktır. Bu yükümlülük tüzel kişiliği temsil ve ilzama yetkili organlar veya kişiler eliyle yerine getirilecektir. Tüzel kişiliği temsil ve ilzama yetkili olan organ veya kişiler tüzel kişilik içerisinde tüzel kişiliğin sahip olduğu veri sorumlusu yükümlülüklerini yerine getirmek üzere kişi veya kişileri görevlendirebilirler. Bu görevlendirme tüzel kişiliğin veri sorumlusu yükümlülüğünü ortadan kaldırmaz ve ilgili gerçek kişilerin de veri sorumlusu olarak tanımlanmasını sağlamaz. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından da Kanunda bir farklılık gözetilmemiştir. Bu çerçevede hukuki ve cezai sorumluluk bakımından, tüzel kişilerin sorumluluğuna ilişkin özel hukuk ve kamu hukukundaki genel hükümler uygulanır.

Veri işleyen, veri sorumlusu adına kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen gerçek veya tüzel kişilerdir. Veri işleyenin faaliyetleri veri işlemenin daha çok teknik kısımları ile sınırlıdır. Burada önemli olan, veri işleyenin bu kapsamdaki kişisel veri işleme faaliyetlerini veri sorumlusundan aldığı talimatlar doğrultusunda gerçekleştirmesidir.

Örneğin, veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına faaliyet gösteren, dışarıdan hizmet alınması suretiyle çağrı merkezi hizmeti veren bir şirket bu faaliyet kapsamında veri işleyen olarak kabul edilecektir.

e-Belediye Bilgi Sistemi

7099 Sayılı Yatırım Ortamının İyileştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun İle; Madde 16- 3/7/2005 tarihli ve 5393 sayılı belediye kanununa aşağıdaki ek madde eklenmiştir.

"Ek Madde 3- belediyeler, mevzuatla kendilerine verilen görev ve hizmetlerin yürütülmesi ve vatandaşlar tarafından yapılan başvuruların sonuçlandırılması amacıyla her türlü idari iş ve işlemin yürütüldüğü e-belediye bilgi sistemini kullanır. e-belediye bilgi sistemini kurmaya, işletmeye, ***veri saklama, veri iletimi ve veri paylaşımı*** *ile ilgili politikaları tespit etmeye, çalışma usul ve esaslarını belirlemeye ve bu sistem ile ilgili merkezî bir hizmet standardizasyonu oluşturmaya içişleri bakanlığı yetkilidir."*

Madde 17- 5393 sayılı kanuna aşağıdaki geçici madde eklenmiştir.

"Geçici Madde 10- belediyeler, e-belediye bilgi sisteminin kurulduğuna dair bildirimin içişleri bakanlığı tarafından yapılmasından itibaren e-belediye bilgi sistemi ile ilgili çalışmaları bir yıl içinde tamamlar. Benzer sistemi kullanan belediyeler, sistemlerinde bulunan ve e-belediye bilgi sistemi için gerekli olan verileri e-belediye bilgi sistemini kullanmaya başladıkları tarihten itibaren bir yıl içinde e-belediye bilgi sistemine aktarır. içişleri bakanı, gerektiğinde bu süreyi bir katına kadar uzatabilir."

Bu düzenlemeler yapılarak e-Belediye Bilgi Sistemi kanunlaşmış ve tüm belediyelerin e-Belediye Bilgi Sistemine dâhil olmasının zorunlu hale geldiği hüküm altına alınmıştır. Buna göre yerel yönetimleri yakından ilgilendiren 6698 sayılı Kişisel Verilerin Korunması Kanunu gereğince e-Belediye Bilgi Sistemi'ne dâhil olan veri sorumlusu belediyeler bakımından Türkiye Cumhuriyeti İçişleri Bakanlığı veri işleyen olarak sorumlu olacaktır. Bilinmelidir ki, veri işleyenin yanı sıra veri sorumlusunun da Kanun'un getirdiği yükümlülükler ve sorumlulukları devam etmektedir.

Kanunda, kişisel veri işleme faaliyetlerine ilişkin hukuki yükümlülüklerin yerine getirilmesinde veri sorumlusu esas alınmaktadır. Veri sorumlusu, kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Veri işleyen ise, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya

tüzel kişidir. Buna göre, veri işleyenin veri sorumlusunun talimatlarını yerine getirdiği açıktır.

Kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesinin, verilere hukuka aykırı olarak erişilmesinin önlemesini ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınması hususunda bu kişilerle birlikte **müştereken sorumludur**. Dolayısıyla veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır.

KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER

Kişisel verilerin işlenmesinde her zaman Kanunda ortaya konulan genel ilkelere uygun davranılmalıdır. Kişisel verilerin işlenmesinde genel ilkeler şunlardır:

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.

Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilmelidir.

Hukuka ve Dürüstlük Kurallarına Uygun Olma

Hukuka ve dürüstlük kuralına uygun olma ilkesi, diğer ilkeleri de kapsayıcı bir özelliğe sahiptir. Hukuka uygun olma, kişisel verilerin işlenmesinde kanunlarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade etmektedir.

Dürüstlük ilkesi ise, ilgili kişi aydınlatılmadan hiçbir şekilde kişisel verisinin toplanmaması ve işlenmemesi, ilgili kişiye karşı haksızlığa yol açacak şekilde kullanılmaması, toplanma amacının aşılmamasını ifade eder. Veri işleme faaliyetinde bulunanların, ilgili kişilerin çıkarlarını ve makul beklentilerini göz önüne almaları

dürüstlük kuralının gereğidir. Haklı bir gerekçe olmaksızın ilgili kişinin özel hayatının gizliliğini, otonomisini, onurunu ihlal edecek şekilde veri işlenmesi, şüphesiz bu ilkeye aykırılık teşkil edecektir. Bu kapsamda, dürüstlük ilkesi uyarınca, kişilerin kendilerine veri işleme konusunda izin ya da emir veren hukuk kurallarına dayanarak gerçekleştirdikleri fiillerde, bu hukuk kuralının amacına göre işlenebilecek en az miktarda veri işlemeleri, veri sahiplerinin öngöremeyeceği biçimde hareket etmemeleri, veri sahiplerinin çıkarlarını ve makul beklentilerini göz önüne almaları gibi davranışları gerektirir.

Bu ilkelere riayet edilmeksizin veri işlenmesi dürüstlük kuralına dolayısıyla hukuka uygun veri işlenmesine aykırı olacaktır.

Doğru ve Gerektiğinde Güncel Olma

Veri, hakkında bilgi vermesi gereken şeyi doğru şekilde anlatabilmelidir. Kişisel verilerin doğruluğunun ve güncelliğinin önemini vurgulayan bu ilke Kanunda öngörülen ilgili kişinin verilerin düzeltilmesini talep etme hakkı ile uyumludur. Kişisel verilerin doğru ve güncel bir şekilde tutulması, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gereklidir.

Veri sorumlusu eğer kişisel verilere dayalı olarak ilgili kişiye dair bir sonuç yaratıyor ise kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında veri sorumlusunun aktif özen yükümlülüğü bulunmaktadır. Bunun dışında veri sorumlusu her zaman ilgili kişinin bilgilerini doğru ve güncel olmasını temin edecek kanalları açık tutmalıdır. Aksi takdirde, kişilerin, güncel olmayan veya yanlış tutulan kişisel verileri nedeniyle maddi ve manevi zarar görmesi mümkündür. Örneğin bir kişinin veri sorumlusunun sisteminde kayıtlı telefon numarasının doğru olmaması ya da artık ilgili kişi tarafından kullanılmıyor oluşu, o kişiye ilişkin gerçek bir veriyi yansıtmadığından hatalı sonuçların ortaya çıkmasına neden olabilmektedir. Yine, adres bilgisi yanlış kaydedilen bir kişinin kendisine ait tebligatları zamanında alamaması veya söz konusu tebligatların yanlış bir kişiye tebliğ edilmesi durumunda ilgili kişi maddi ve manevi zarar görebilir.

Kişisel verilerin doğru ve güncel tutulabilmesini teminen; kişisel verilerin elde edildiği kaynaklar belirli olmalı, kişisel verilerin toplandığı kaynağın doğruluğu test

edilmeli, kişisel verilerin doğru olmamasından kaynaklı talepler göz önünde bulundurulmalı ve bu kapsamda makul önlemler alınmalıdır.

Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

Kişisel verilerin işlenme amaçlarının belirli, meşru ve açık olması ilkesi;

• Kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılabilir olmasını,
• Kişisel veri işleme faaliyetlerinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini,
• Kişisel veri işleme faaliyetinin ve bu faaliyetin gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlamaktadır.

Kişisel veri işleme amaçlarının belirli, meşru ve açık olması ilkesi özellikle açık rıza ve aydınlatma metinlerinin kaleme alınması sırasında; kişisel veri işleme faaliyetlerinin hukuka uygun olarak gerçekleştirildiğinin tespitinin sağlanması noktasında önem taşır. Açıklandığı hukuki işlem ve metinlerde (açık rıza, aydınlatma, ilgili kişinin başvurularını cevaplama, veri sorumlusu siciline olan başvuru) belirlilik ve açıklık ilkesine uyumda hassasiyet gösterilmesi, anlaşılmayan terminoloji kullanımından kaçınılmasıdır. Bu esasa uygun davranma aynı zamanda dürüstlük ilkesine uyum bakımından da önemlidir.

Amacın Meşru Olması İlkesi

Amacın meşru olması; veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Örneğin, bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi meşru amaç kapsamındayken, anne kızlık soyadını işlemesi meşru amaç kapsamında değerlendirilemeyecektir.

Kişisel Verilerin, İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması İlkesi

"Amaçla sınırlılık" kişisel verilerin korunmasında hâkim olan en önemli ilkelerden biridir. Kişisel veriler işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Mevcutta olmayan ve sonradan gerçekleşmesi düşünülen amaçlarla kişisel veri toplanmamalıdır. Kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan

ölçüde kişisel veri toplanmamalı ve/ veya işlenmemelidir. Buna göre kişisel veriler yalnızca belirli amaçlar için ve gerektiği kadar toplanmalı, amacın gerektirdiği yerlerde kullanılmalıdır.

Bu bakımdan, kişisel veriler toplandıktan sonra, ileride ortaya çıkabilecek yeni işleme amaçları dâhilinde işleme yapılması için, verilerin ilk defa toplanması sırasında sağlanması gereken şartlar yeni amaçlar için de tekrar aranmalıdır. Örneğin, bir taşımacılık firması tarafından taşıma sözleşmesi kapsamında kaydedilen adres bilgileri, sonrasında pazarlama faaliyeti için de kullanılacaksa, bu amaçla kullanım yapılabilmesi için kişisel veri işleme şartlarının karşılanıp karşılanmadığının yeniden değerlendirilmesi gerekmektedir.

Bunun yanı sıra işlenen veri, sadece veri işleme amacının gerçekleştirilmesi için gerekli olanla sınırlı tutulmalıdır. Örneğin, bir tekstil firması tarafından müşterilere ilişkin kimlik ya da iletişim verilerinin tutulması satış işlemlerinin takibi vb. amaçlarla bağdaşırken, müşterilerin finansal geçmişine ilişkin verilerin toplanmasının amaçla bağlantılı ve ölçülü olduğu söylenemez.

Bunun yanında amaçla bağlantılı, sınırlı ve ölçülü olma şartının her ilgili kişi ve süreç için ayrı ayrı değerlendirilmesi gerekmektedir. Çünkü belirli bir kişi ve süreç için gerekli olan bilgi, bir diğer kişi için ölçüsüz olabilecektir. Bu hususa özellikle özel nitelikli kişisel veriler konusunda dikkat edilmesi gerekir. Bir iş yerinde insan kaynakları birimince çalışanların mali haklarının belirlenebilmesi için sendika üyeliği verisinin alınması ölçülü kabul edilecekken, aynı iş yerinin AR-GE birimince söz konusu verinin alınması ölçülü olarak kabul edilmeyecektir.

Kişisel Verilerin Ancak İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilmesi

Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. Buna göre, veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak, kişisel verileri ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep bulunmaması halinde, o veri silinecek, yok edilecek ya da anonim hale getirilecektir. İleride tekrar kullanılabileceği düşünülerek ya da herhangi bir başka gerekçe ile kişisel verilerin muhafaza edilmesi yoluna gidilemeyecektir.

Ayrıca veri sorumlusu, Kanunun 16. maddesi uyarınca Veri Sorumluları Siciline kayıt için başvuru yaparken kişisel verilerin işlenme amacı için gerekli azami süreyi bildirmek zorundadır.

Veri sorumlusu tarafından Sicile bildirilen veri kategorilerinin işleme amaçları ve bu amaçlara dayalı olarak işlenmeleri için gerekli olan azami muhafaza edilme süreleri ile mevzuatta öngörülen süreler farklı olabilir. Bu durumda mevzuatta azami muhafaza edilme süresi öngörülmüşse öngörülen bu süre yoksa bunlardan en uzun süre esas alınarak bu veri kategorisi için Sicile bildirim yapılır.

Burada önemle belirtmek gerekir ki, mevzuat kapsamında öngörülen bu sürelere uyum için yapılan saklama faaliyetleri veri sorumlusu tarafından belirlenen saklama sürelerini aşıyorsa, bu faaliyetler yalnızca ilgili mevzuatta belirtilen yükümlülükleri yerine getirmekle sınırlı bir saklama ve işleme faaliyeti olarak yürütülmelidir. Hem veri sorumlusunun hukuki yükümlülükleri gereği tabi olduğu mevzuat kapsamında öngörülen sürelerin, hem de veri sorumlusunun belirlediği saklama sürelerinin aşılması durumunda, kişisel verilerin veri sorumlusu tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmeliğe göre silinmesi, yok edilmesi veya anonim hale getirilmesinin temin edilmesi gerekir.

KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Kanunun 5. maddesinde kişisel verilerin işlenme şartları düzenlenmiştir. Özel nitelikli kişisel verilerin işlenme şartları ise Kanunun 6. maddesinde farklı esaslara bağlanmıştır. Bu çerçevede, özel nitelikli olmayan kişisel verilerin hangi hallerde hukuka uygun olarak işlenebileceği Kanundaki esaslara göre aşağıdaki şekilde düzenlenmiş olup, bu şartlardan sadece bir tanesinin bulunması özel nitelikli olmayan kişisel verilerin işlenmesi için yeterli hukuki şartı oluşturacaktır.

1. İlgili kişinin açık rızasının varlığı,
2. Kanunlarda açıkça öngörülmesi,
3. 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,
4. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

5. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
6. İlgili kişinin kendisi tarafından alenileştirilmiş olması,
7. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
8. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel verilerin işlenme şartları, yani hukuka uygunluk halleri, Kanunda sınırlı sayıda sayılmış olup, bu şartlar genişletilemez.

Kişisel veri işleme, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmamaktadır. Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim, ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelecektir.

Herhangi bir şekilde ilgili kişi tarafından kamuoyuna açıklanmış olan bir başka ifadeyle ilgili kişinin kendisi tarafından alenileştirilen kişisel verileri alenileştirme amacına uygun bir şekilde açık rıza aranmaksızın işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.

Kişisel verinin, aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir. Başka bir ifade ile alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gerekir. Yoksa bir kişinin kişisel verisinin herkesin görebileceği bir yerde olması aleni olmasını sağlamaz. Ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir. Örneğin, ikinci el araç satışı yapılan internet sitelerinde aracını satmak isteyen ilgili kişinin iletişim bilgilerinin pazarlama amaçlarıyla kullanılması mümkün değildir.

Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Özel nitelikli kişisel veriler öğrenilmesi halinde ilgili kişiler hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle, diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir.

Kanun, bu verilere özel bir önem atfetmekte ve bu verilerle ilgili farklı bir düzenleme getirmektedir. Kanun bunları özel nitelikli kişisel veri ya da hassas veriler olarak kabul etmektedir. Özel nitelikli kişisel veriler ilgili kişinin açık rızası ile ya da Kanunda sayılan sınırlı hallerde işlenebilir.

Kanun, özel nitelikli kişisel veriler arasında da bir ayrım yapmıştır. Buna göre sağlık ve cinsel hayata ilişkin kişisel veriler ile bunlar dışındaki özel nitelikli kişisel verilerin, açık rıza olmaksızın işlenebileceği haller, Kanunda farklı düzenlenmiştir.

Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, 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.

Belirtmek gerekir ki, bütün durumlarda, özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliğin 4. maddesinde ilgili kullanıcı; "verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler" olarak tanımlanmıştır.

Buna göre ilgili kullanıcı, veri sorumlusu uhdesinde olmakla birlikte verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan arşiv sorumlusu ve/veya veri tabanı yöneticisi gibi bir kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde yer alan tüm çalışanlar ve birimler ya da veri sorumlusundan aldığı yetki ve talimat ile bu alanda hizmet veren üçüncü kişiler gibi veri işleyenleri tanımlamaktadır.

Örneğin bir veri sorumlusu ile bilgi işlem altyapısı iş ve işlemlerini onun yetki ve talimatları çerçevesinde yerine getirmek üzere anlaşma yapmış olan ve bu konuda çalışan bir firma veri işleyen sayılacaktır. Bu durumda bu veri sorumlusunun veri tabanı yöneticiliği yapan birim ya da personeli bulunmuyorsa tüm çalışanları ilgili kullanıcı olacaktır. Ayrıca veri işleyen firmanın da veri tabanı yöneticisi hariç geri kalan tüm çalışanları da ilgili kullanıcı kavramı içerisinde yer alacaktır. Kişisel verilerin silinmesi ve yok edilmesi arasındaki fark da ilgili kullanıcı kavramına göre şekillenmiştir.

Yok etme, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyalar tespit edilir ve verilerin bulunduğu sistemlerin türüne göre de-manyetize etme, fiziksel yok etme, üzerine yazma gibi yöntemlerden bir ya da bir kaçı kullanılır.

Anonim hale getirme kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Diğer bir ifade ile anonim hale getirme bir veri kümesindeki tüm doğrudan ve dolaylı tanımlayıcıların çıkarılarak veya değiştirilerek ilgili kişinin kimliğinin saptanabilmesinin engellenmesi ya da bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişi ile ilişkilendirilemeyecek şekilde kaybetmesidir. Bu kapsamda, veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabiliyorsa, bu verinin anonim hale getirildiği kabul edilemez.

Anonim hale getirilen veri artık kişisel veri niteliklerine sahip olmayacağından, Kanun hükümleri kapsamında değerlendirilemeyecektir. Veri setleri anonim hale getirilme işlemlerine tabi tutuldukları ana kadar kişisel veri niteliklerine sahip olduklarından, bu veriler üzerinde gerçekleştirilecek her türlü işlem kişisel verilerin işlenmesi olarak kabul edilmektedir.

Anonim veri başından beri belirli bir kişiyle ilişkilendirilmesi mümkün olmayan veriyi ifade ederken, anonim hale getirilmiş veri daha öncesinde bir kişiyle ilişkilendirilmiş ancak artık bağlantısı kalmamış veridir.

Kişisel Verilerin Yurtiçinde Aktarılması

Kanunda yer alan kişisel verilerin işlenmesine ilişkin şartların tamamının ortadan kalkması durumunda kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

Kanunda, kişisel verilerin ilgilinin açık rızası olmak şartıyla üçüncü kişilere aktarılabileceği öngörülmektedir. Bununla birlikte, Kanunun 5. ve 6. maddesindeki şartların sağlanması halinde yeterli önlemler alınarak kişisel verilerin açık rıza aranmaksızın yurtiçinde aktarılmasına da imkân tanınmıştır. Bu kapsamda;

1.Kişisel veriler açısından Kanunun 5. maddesinin 2. fıkrasında sayılan işleme şartlarından en az birinin bulunması,

2.Özel nitelikli kişisel veriler açısından ise yeterli önlemler alınmak kaydıyla Kanunun 6.maddesinin 3. fıkrasında belirtilen şartlardan birinin bulunması halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin aktarılması mümkündür.

Kişisel Verilerin Yurt Dışına Aktarılması

Kanunun 9. maddesinin 1. fıkrasında kişisel verilerin ilgili kişinin açık rızası olmak şartıyla yurt dışına aktarılabileceği düzenlenmiştir. Bununla birlikte maddenin 2. fıkrasında, Kanunun 5. maddesinin 2. fıkrası kapsamındaki kişisel veriler ile 6. maddesinin 3. fıkrasında belirtilen özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenmesine izin veren şartlar esas alınmakta ve bu şartlardan birinin varlığı halinde, kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunması kaydıyla, ilgili kişinin açık rızası aranmaksızın kişisel verilerin yurt dışına aktarılmasına imkân tanındığı belirtilmektedir. Buna göre;

1. İlgili kişinin açık rızasının bulunması
2. Kanunun 5. maddesinin 2. fıkrasında ve Kanunun 6. maddesinin 3. fıkrasında belirtilen şartlardan birinin bulunması ve verinin aktarılacağı ülkede;
   a)Yeterli korumanın bulunması,

b)Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla kişisel verilerin yurt dışına aktarılması mümkündür.

Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilecektir. Bu kapsamda, yabancı ülkede yeterli koruma bulunup bulunmadığına ve yeterli koruma bulunmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı taahhüt etmeleri şartıyla söz konusu kişisel verilerin yurtdışına aktarılıp aktarılmayacağına Kurul tarafından karar verilecektir.

İlave olarak, Kanunun 9. maddesinin 5. fıkrasında kişisel verilerin, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum ve kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabileceği hükme bağlanmıştır.

Aydınlatma Yükümlülüğü

Veri sorumlusu veya yetkilendirdiği kişi, aydınlatma yükümlülüğü kapsamında veri sorumlusunun ve varsa temsilcisinin kimliği, veri işleme amacı, işlenen verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile Kanunun 11. maddesinde sayılan diğer hakları konusunda ilgili kişiyi bilgilendirmekle yükümlüdür. Aydınlatma yükümlülüğünün yerine getirilmesi ilgili kişinin onayına tabi değildir.

Kişisel veri işleme faaliyeti kapsamında kişisel verinin elde edilmesi sırasında veri sorumlusu tarafından ilgili kişilerin aydınlatılması gerekmektedir. Bununla birlikte aydınlatma yükümlülüğü yerine getirilirken ilgili kişiye verilecek bilgiler, eğer Veri Sorumluları Siciline kayıt yükümlülüğü varsa, Veri Sorumluları Siciline açıklanan bilgilerle uyumlu olmalıdır. Kayıt yükümlüğü yoksa Kanunun 10. ve 11. maddeleri kapsamında aydınlatma yükümlülüğü yerine getirilmelidir.

Veri işleme faaliyetinin ilgili kişinin açık rızasına bağlı olmadığı ve faaliyetin Kanundaki başka şartlar kapsamında yürütüldüğü durumlarda da veri sorumlusunun ve yetkilendirdiği kişinin ilgili kişiyi aydınlatma yükümlülüğü devam etmektedir.

Aydınlatma yükümlülüğünün yerine getirilmesi konusunda bir şekil şartı bulunmamaktadır. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı ise veri sorumlusuna aittir.

İlgili Kişinin Hakları

Kanunun 11. maddesi çerçevesinde herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a. Kişisel verilerinin işlenip işlenmediğini öğrenme,
b. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c. Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç. Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d. Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e. Kanunun 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f. Maddenin (d) ve (e) bentlerinde belirtilen düzeltme, silme ve yok etme talepleri doğrultusunda yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ. Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

YÜKÜMLÜLÜKLER

6698 sayılı Kişisel Verilerin Korunması Kanunu gereğince veri sorumlularına bir takım yükümlülükler getirilmiştir. Buna göre veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek ile verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Ayrıca, veri sorumlusu, kurum ve kuruluşunda Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak ve yaptırmak zorundadır.

Veri sorumluları öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkalarına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülükleri görevden ayrılmalarından sonra da devam eder. Öte yandan, veri sorumluları için düzenlenen sır saklama yükümlülüğü Kanunda veri işleyenler için de getirilmiştir.

Veri sorumlusunun bir diğer yükümlülüğü ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde de veri sorumlusunun bu durumu Kurula bildirme yükümlülüğüdür. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yolla ilan eder.

Kanunun 3. maddesinde, veri sorumlusu "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmıştır.

Veri sorumlusu, kişisel verileri bizzat işleyebileceği gibi, veri işleme faaliyetini gerçekleştirmek üzere üçüncü bir kişiyi de yetkilendirebilir. Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen bu tür gerçek veya tüzel kişiler, Kanunun 3. maddesinin 1. fıkrasının (ğ) bendinde "veri işleyen" olarak adlandırılmıştır. Kanunda kişisel verilerin korunmasına ilişkin bazı yükümlülükler, veri sorumluları ile birlikte veri işleyenler için de getirilmiştir.

Veri sorumlusunun kanun kapsamında pek çok yükümlülüğü bulunmakla birlikte bunlardan bazıları aşağıda ayrıntılı olarak açıklanmaktadır:

Aydınlatma Yükümlülüğü

Kanun koyucu kişisel verileri işlenen ilgili kişilere bu verilerinin kim tarafından, hangi amaçlarla ve hukuki sebeplerle işlenebileceği, kimlere hangi amaçlarla aktarılabileceği hususunda bilgi edinme hakkı tanımakta ve bu hususları, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ele almaktadır. Buna göre veri sorumlusu, Kanunun 10. maddesi çerçevesinde kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aşağıdaki bilgileri ilgili kişiye sağlamakla yükümlüdür:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- 11. maddede sayılan diğer hakları.

Öte yandan, 10.03.2018 tarihli Resmi Gazetede yayımlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" ile aydınlatma yükümlülüğü kapsamında veri sorumlularınca uyulması gereken usul ve esaslar konusunda düzenleme yapılmış olup, veri sorumlularınca aydınlatma yükümlülüğü yerine getirilirken bu hususlara da dikkat edilmesi gerekecektir.

Veri işleme faaliyetinin ilgili kişinin açık rızasına bağlı olduğu veya faaliyetin Kanundaki diğer bir şart kapsamında yürütüldüğü durumlarda da veri sorumlusunun ilgili kişiyi bilgilendirme yükümlülüğü devam etmektedir. Yani ilgili kişi, kişisel verisinin işlendiği her durumda aydınlatılmalıdır.

Veri Sorumluları Siciline kayıt yükümlülüğünün bulunması durumunda aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır. Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin onayına tabi değildir. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı ise veri sorumlusuna aittir.

Veri Güvenliğine İlişkin Yükümlülükler

Kanunun veri güvenliğine ilişkin 12. maddesine göre veri sorumlusu;

• Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
• Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
• Kişisel verilerin muhafazasını sağlamak,
ile yükümlüdür.

Veri sorumlusu bu yükümlülüklerini yerine getirmek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Ayrıca, veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak ise Kurulun yetki ve görevleri arasında yer almaktadır.

Bununla birlikte, Kurul tarafından belirlenecek asgari kriterler esas alınmak üzere sektör bazında işlenen kişisel verilerin niteliğine göre ilave tedbirlerin alınması da söz konusu olabilecektir.

Maddenin devamında, veri sorumlusunun, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu belirtilmiştir. Dolayısıyla veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır. Buna göre, örneğin veri sorumlusunun şirketine ilişkin kayıtlar bir muhasebe şirketi tarafından tutuluyorsa, verilerin işlenmesine ilişkin birinci fıkrada belirtilen tedbirlerin alınması hususunda veri sorumlusu muhasebe şirketiyle birlikte müştereken sorumlu olacaktır.

Kanunda, veri güvenliğine ilişkin olarak ayrıca veri sorumlusuna denetim yükümlülüğü getirilmiştir. Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Kanun denetimin veri sorumlusu tarafından yapılması gerektiğini öngörmektedir. Veri sorumlusu bu denetimi kendisi gerçekleştirebileceği gibi, bir üçüncü kişi vasıtasıyla da gerçekleştirebilir.

Öte yandan, veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

Son olarak, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir.

Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

Veri güvenliğine ilişkin alınacak önlemlerin her bir veri sorumlusunun yapısına, faaliyetlerine ve tabi olduğu risklere uygun olması gerekmektedir. Bu nedenle, veri güvenliğine ilişkin tek bir model öngörülememektedir. Uygun önlemlerin belirlenmesinde şirketin büyüklüğü veya cirosunun yanı sıra veri sorumlusunun yaptığı işin ve korunan kişisel verinin niteliği de önemlidir. Örneğin, küçük ölçekli olmakla birlikte özel nitelikli kişisel veri işleyen veri sorumlusunun daha yüksek standartlarda koruma önlemi alması gerekmektedir.

İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması ve Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü

Kanunun 13. maddesine ve bu maddeye istinaden 10.03.2018 tarihli Resmi Gazetede yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe göre veri sorumluları, ilgili kişiler tarafından yazılı olarak veya bahse konu Tebliğ'de yer verilen kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla yapılan başvuruları niteliklerine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır.

Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, veri sorumlusu, Kurulca belirlenen tarifedeki ücretleri başvuruda bulunan ilgili kişiden isteyebilir.

Veri sorumlusu, talebi kabul eder ise veya gerekçesini açıklayarak reddeder ise bu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusu tarafından bu talebin gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde ise alınan ücret ilgiliye iade edilir.

Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını

öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda yapacağı inceleme sonucunda bir ihlalin varlığını tespit ederse, hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek, kararı ilgililere tebliğ eder. Veri sorumlusu, bu kararı, tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirmek zorundadır.

Veri Sorumluları Siciline Kaydolma Yükümlülüğü

Kanunun 16. maddesine göre, Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacaktır. Yine bu maddeye göre kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce bu Sicile kaydolmak zorundadır.

Ancak, Kanunun 16. maddesinin 2. fıkrasında, 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 getirilebileceği belirtilmiştir.

Bu hükme istinaden Kurul tarafından söz konusu kriterler belirlenmiş ve 30.12.2017 tarihli Resmi Gazetede yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelikte bu kriterler sayılmıştır. Söz konusu kriterler:

a) Kişisel verinin niteliği.
b) Kişisel verinin sayısı.
c) Kişisel verinin işlenme amacı.
ç) Kişisel verinin işlendiği faaliyet alanı.
d) Kişisel verinin üçüncü kişilere aktarılma durumu.
e) Kişisel veri işleme faaliyetinin kanunlardan kaynaklanması.
f) Kişisel verilerin muhafaza edilmesi süresi.
g) Veri konusu kişi grubu veya veri kategorileri.

Bildirim Yükümlülüğü

Veri sorumlusunun diğer bir yükümlülüğü de işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurula bildirmektir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

Belediyeleri de ilgilendiren Kurul Kararı

Banko, Gişe, Masa Gibi Birden Fazla Çalışan ile Bitişik Düzende Hizmet Veren Kurumlar Hakkında Kişisel Verileri Koruma Kurulu 2017/62 Sayılı İlke Kararına göre, banko, gişe ve masa gibi vatandaşa hizmet sunulan alanlarda yaşanan kişisel veri güvenliği ihlallerine ilişkin olarak Kişisel Verileri Koruma Kurumu'na intikal eden ihbarlar değerlendirilmiş ve uygulamada yaşanan problemlerin önüne geçilmesi amacıyla aşağıdaki karar alınmıştır.

2017/62 Sayılı Kişisel Verileri Koruma Kurulu Kararı'nda, bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile **belediye**, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşları, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12'nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirilerine yakın konumda hizmet alanların birbirilerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri alacaktır.

İDARİ TEDBİRLER

İDARİ TEDBİRLER ÖZET TABLOSU
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Sakalam ve İmha vb.)
Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Bu riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm

alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.

Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.

Kişisel veri güvenliğini ihlal etmeye yönelik saldırıların yanı sıra, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu ihlaller, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinin kullanılması suretiyle kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde de ortaya çıkabilmektedir.

Bu nedenle çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.

Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.

Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesine dikkat edilmelidir.

Öte yandan, çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşmalarını imzalamaları istenebilir. Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci de mutlaka olmalıdır.

Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; yapılacak yeni eğitimlerle bu değişikliklerin, çalışanların bilgisine sunulması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulması sağlanmalıdır.

Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

Kişisel veri güvenliğine ilişkin iyi bir politika hazırlanması, bu kapsamdaki risklerin önceden belirlenebilmesini ve istikrarlı bir şekilde önlem alınmasını sağlayacaktır.

Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılamadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır.

Bu kapsamda alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetimi, çalışanlar üzerinde ortaya çıkabilecek baskıyı azaltacaktır. Bu nedenle veri sorumlularının, veri kayıt sistemlerinde hangi kişisel verilerin bulunduğundan ve mevcut güvenlik önlemlerini inceleyerek diğer yasal yükümlülüklerle uyumlu hareket edildiğinden emin olması gerekmektedir.

Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.

Ayrıca, her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.

Kişisel Verilerin Mümkün Olduğunca Azaltılması

Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Ancak, özellikle uzun süredir faaliyet gösteren veri sorumluları, çok fazla miktarda kişisel veri toplamakta olduğundan söz konusu kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir. Bunun önüne geçebilmek için, veri sorumlularınca işleme amaçları bakımından anılan kişisel verilere hala ihtiyaç olup olmadığının değerlendirilmesi ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olunması gerekmektedir.

Bunun yanında, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmekte ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

Veri İşleyenler ile İlişkilerin Yönetimi

Bazı veri sorumluları, bilgi teknolojileri ihtiyaçlarını karşılamak için veri işleyenlerden hizmet almaktadırlar. Veri sorumlularının, hizmet alırken söz konusu veri işleyenlerin kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin sağlandığından emin olmaları gerekmektedir. Zira Kanunun 12 nci maddesinin ikinci fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur.

Veri işleyen ile imzalanan sözleşmenin yazılı olması, veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hüküm içermesi ve Kişisel Veri Saklama ve İmha Politikasına uygun olması önerilmektedir.

Veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağının da bu sözleşmede yer alması önem taşımaktadır.

Yine söz konusu sözleşmede herhangi bir veri ihlali olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olduğunun öngörülmesi de, veri sorumlusunun bu ihlali derhal Kişisel Verileri Koruma Kurulu'na ve ilgili kişiye bildirme yükümlülüğünü yerine getirmesi açısından faydalı olacaktır.

Ayrıca; taraflar arasındaki sözleşmenin niteliği buna elverdiği ölçüde, veri sorumlusu tarafından veri işleyene aktarılan kişisel veri kategori ve türlerinin de ayrı bir maddede belirtilmiş olması, veri işleyenin veri güvenliğini sağlama yükümlüğünü yerine getirmesi açısından faydalı olacaktır.

Bununla birlikte veri sorumlusu, kişisel veri içeren sistem üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir.

KİŞİSEL VERİ İŞLEME ENVANTERİ ÖRNEĞİ													
	ORGANİZASYON	SÜREÇ	KİŞİSEL VERİ						SAKLAMA ve İMHA	AKTARMA		ALINAN GÜVENLİK TEDBİRLERİ	
	Departman	Faaliyet	Veri Kategorisi	Kisisel Veri	Özel Nitelikli Kişisel Veri	İşleme Amacı	Veri Konusu Kişi Grubu	Hukuki Sebebi	Saklama Süresi	Alıcı / Alıcı Grupları	Yabancı Ülkelere Aktarılan Veriler	İdari Tedbirler	Teknik Tedbirler
1	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Kimlik	Ad, Soyad		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışanlar	Sözleşme İmzalanması	İşten Ayrılmasından İtibaren 10 yıl	SGK Ve Diğer Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor	"Çalışanların Niteliği Ve Teknik Bilgi/ Becerisinin Geliştirilmesi, Kişisel Verilerin Hukuka Aykırı İşlenmenin Önlenmesi, Kişisel Verilere Hukuka Aykırı Erişilmesinin Önlenmesi, Kişisel Verilerin Muhafazasının Sağlanması, İletişim Teknikleri Ve İlgili Mevzuatlar Hakkında Eğitimler Verilmekte; Çalışanlara Gizlilik Sözleşmeleri İmzalatılmakta; Güvenlik Politika Ve Prosedürlerine Uymayan Çalışanlara Yönelik Uygulanacak Disiplin Prosedürü Uygulanmakta, İlgili Kişileri Aydınlatma Yükümlülüğü Yerine Getirilmekte, Kurum İçi Periyodik Ve Rastgele Denetimler Yapılmakta Ve Çalışanlara Yönelik Bilgi Güvenliği Eğitimleri Verilmektedir."	"Kurumun Bilişim Sistemleri Teçhizatı, Yazılım Ve Verilerin Fiziksel Güvenliği İçin Gerekli Önlemler Alınmakta, Hukuka Aykırı İşlemeyi Önlemeye Yönelik Riskler Belirlenmekte, Bu Risklere Uygun Teknik Tedbirler Alınmakta, Erişim Yetki Ve Rol Dağılımları İçin Prosedürler Oluşturulmakta Ve Uygulanmakta, Yetki Matrisi Uygulanmakta, Erişimler Kayıt Altına Alınarak Uygunsuz Erişimler Kontrol Altında Tutulmakta, Saklama Ve İmha Politikasına Uygun İmha Süreçleri Tanımlanmakta Ve Uygulanmakta, Hukuka Aykırı İşleme Tespiti Halinde İlgili Kişiye Ve Kurula Bildirmek İçin Bir Sistem Ve Altyapı Oluşturulmakta, Güvenlik Açıkları Takip Edilerek Uygun Güvenlik Yamaları Yüklenmekte, Bilgi Sistemleri Güncel Halde Tutulmakta, Kişisel Verilerin İşlendiği Elektronik Ortamlarda Güçlü Parolalar Kullanılmakta Ve Güvenli Kayıt Tutma (Loglama) Sistemleri Kullanılmakta, Kişisel Verilerin Güvenli Olarak Saklanmasını Sağlayan Yedekleme Programları Kullanılmaktadır."
2	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Kimlik	TC Kimlik No		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışanlar	Sözleşme İmzalanması	İşten Ayrılmasından İtibaren 10 yıl	SGK Ve Diğer Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		
3	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	İletişim	Telefon Numarası		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışanlar	Sözleşme İmzalanması	İşten Ayrılmasından İtibaren 10 yıl	Aktarılmıyor	Yurt dışına Aktarım Yapılmıyor		
4	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Kimlik	Anne – Baba Adı		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışanlar	Sözleşme İmzalanması	İşten Ayrılmasından İtibaren 10 yıl	SGK Ve Diğer Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		
5	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Eğitim	KPSS Puanı		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışanlar	Kanunlarda Öngörülmesi	İşten Ayrılmasından İtibaren 10 yıl	Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		
6	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Kimlik	Bakmakla Yükümlü Olduğu Kişilerin Ad Ve Soyad Bilgisi		Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi	Çalışan ve Çalışan Yakınları	Kanunlarda Öngörülmesi	İşten Ayrılmasından İtibaren 10 yıl	SGK Ve Diğer Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		
7	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Özlük	İzin Bilgisi		İnsan kaynakları süreçlerinin yürütülmesi	Çalışanlar	Kanunlarda Öngörülmesi	İşten Ayrılmasından İtibaren 10 yıl	Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		
8	İnsan Kaynakları	Çalışan Özlük Dosyası Oluşturma	Özlük	Mal Bildirimi Beyanı		Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	Çalışan ve Çalışan Yakını	Kanunlarda Öngörülmesi	İşten Ayrılmasından İtibaren 10 yıl	Yetkili Kurum ve Kuruluşlar	Yurt dışına Aktarım Yapılmıyor		

Şekil 1 Kişisel Veri İşleme Envanteri Örneği

TEKNİK TEDBİRLER

TEKNİK TEDBİRLER ÖZET TABLOSU
Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

Siber Güvenliğin Sağlanması

Kişisel veri güvenliğinin sağlanması için tek bir siber güvenlik ürünü kullanımı ile tam güvenliğin sağlanabileceği görüşü her zaman doğru değildir. Çünkü tehditler her geçen gün boyut ve nitelik değiştirerek etki alanlarını genişletmektedirler.

Bu kapsamda tavsiye edilen yaklaşım, birçok prensip dahilinde tamamlayıcı niteliğe sahip ve düzenli olarak kontrol edilen birtakım tedbirlerin uygulanmasıdır.

Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, güvenlik duvarı ve ağ geçididir. Bunlar, internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattı olacaktır.

İyi yapılandırılmış bir güvenlik duvarı, kullanılmakta olan ağa derinlemesine nüfuz etmeden önce, gerçekleşen ihlalleri durdurabilir. İnternet ağ geçidi ise çalışanların, kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önleyebilir.

Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir.

Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir.

Ayrıca, kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmalıdır. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmalıdır.

Buna bağlı olarak veri sorumlularının, erişim yetki ve kontrol matrisi oluşturmaları ve ayrı bir erişim politika ve prosedürleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınması önerilmektedir.

Güçlü şifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin

sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişikleri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılması gerekmektedir.

Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.

Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanması için önemlidir.

Kişisel Veri Güvenliğinin Takibi

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir.

Bu durumun önüne geçebilmek için;

a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,

b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,

c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),

ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,

d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir.

Söz konusu raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir.

Ayrıca güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir.

Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunması gerekmektedir. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınması önemlidir.

Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.

Aynı seviyedeki önlemlerin veri sorumlusu yerleşkesi dışında yer alan ve veri sorumlusuna ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir.

Kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi gerekmektedir. Ayrıca çalışanların şahsi

elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için de mutlaka yeterli güvenlik tedbirleri alınmalıdır.

Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler de alınmalıdır.

Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmalı, söz konusu evraklara yetkisiz erişim önlenmelidir.

Bunlarla birlikte şifreleme farklı farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracıdır. Bu kapsamda, tam disk şifrelemesiyle cihazın tümü şifrelenebilir ya da cihazda bulunan bir dosya şifrelenebilir. Bazı yazılımlar ise verilerde değişiklik yapılmasına izin vermemek için şifre koruması sunmakla birlikte bu yazılımlar kişisel verinin yetkisiz kişiler tarafından okunmasını durdurmaz. Bu nedenle hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir. Tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem gösterilmelidir.

Kişisel Verilerin Bulutta Depolanması

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü olan veri sorumlusunun kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu durum birtakım riskleri beraberinde getirmektedir.

Bu nedenle, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusunca değerlendirilmesi gerekmektedir.

Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir.

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir.

Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekir.

Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

Veri sorumlusu tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır.

Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır.

Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılması gerekir. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir.

Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir. Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir.

Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmalıdır.

VERBİS - VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ

Veri Sorumluları Sicili (VERBİS), veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir. Veri sorumlularının, Kurulun gözetiminde Başkanlık tarafından tutulmakta olan Veri Sorumluları Siciline kaydolmaları zorunludur. Dolayısıyla veri sorumlularının kimler olduğunun kamuya açıklanması ve bu yöntemle kişisel verilerin korunması hakkının daha etkin şekilde kullanılması hedeflenmektedir.

Kişisel veri işleme faaliyeti kapsamında kişisel verinin elde edilmesi sırasında veri sorumlusu tarafından ilgili kişilerin aydınlatılması gerekmektedir. Bununla birlikte aydınlatma yükümlülüğü yerine getirilirken ilgili kişiye verilecek bilgiler, eğer Veri Sorumluları Siciline kayıt yükümlülüğü varsa, Veri Sorumluları Siciline açıklanan bilgilerle uyumlu olmalıdır.

Veri Sorumluları Siciline kayıt olmak için başvuru, aşağıdaki bilgileri içeren bir bildirim ile yapılacaktır. Söz konusu bilgiler şunlardır:

- Veri sorumlusu ve varsa temsilcisinin 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,
• Yabancı ülkelere aktarımı öngörülen kişisel veriler,
• Kişisel veri güvenliğine ilişkin alınan tedbirler,
• Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

Yukarıda listelenen bilgilerde herhangi bir değişiklik olması halinde, söz konusu değişikliklerin derhal Kuruma bildirilmesi gerekmektedir. Böylelikle, Sicilin güncelliğinin sağlanması hedeflenmiştir.

Unutulmamalıdır ki; veri sorumlusu kurum veya kuruluş, 6698 sayılı Kanun'un getirdiği yükümlülükleri tamamlamadan, veri güvenliği önlemlerini almadan, envanterini ortaya çıkarmadan VERBİS kaydı yapmamalıdır.

Veri Sorumluları	**Kayıt Yükümlülüğü Başlangıç Tarihi**	**Kayıt Yükümlülüğü Son Tarihi**
Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları	01.10.2018	30.06.2020
Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları	01.10.2018	30.06.2020
Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları	01.01.2019	30.09.2020
Kamu kurum ve kuruluşu veri sorumluları	01.04.2019	**31.12.2020**

Veri sorumlusu VERBİS'e kayıt yaparken bir irtibat kişisi belirlemek zorundadır. Kamu kurum ve kuruluşlarında, belediyelerde irtibat kişisi, üst düzey yönetici tarafından Kurum ile iletişimi sağlamak amacıyla belirlenerek Sicile kaydı yapılan daire başkanı veya üstü yöneticidir.

VERBİS kaydı yapılırken sicile açıklanan bilgilerin kurumun kişisel veri işleme envanterine uygun olması gerekmektedir. Bu nedenle öncelikle kurumun veri yaşam döngüsü belirlenmeli, veri tasnifi yapılmalı ve kurumsal politikalar belirlenmelidir.

Örneğin belediyeler için kişisel verilerin saklama süreleri ilgili mevzuatlara göre belirlenmelidir. Belediyeler, Kanunların kendisine verdiği yetki ve görevleri yerine getirmek için yaptığı faaliyetler sonucunda belge üretmektedir. Kişisel veri içeren bu belgeler, belediyelerin varlık sebebini ortaya koyan temel dayanaklarıdır. Belediyelerin görev ve hizmetleri neticesinde oluşan belgelerin güncelliğini kaybetmesinin ardından toplumun istifadesine sunulması da Devlet arşiv hizmetlerinin bir gereğidir. Bunun gerçekleştirilebilmesi, belediyelerin iş ve işlemleri sonucunda teşekkül eden belgelerin arşivcilik metod ve tekniklerine uygun olarak düzenlenmesi ve korunması ile mümkündür.

Günümüze kadar birikmiş olan belgelerin ayıklanması için de yine kurum arşiv sorumlusunun başkanlığında ayıklama ve imha komisyonları teşkil ettirilerek, ayıklama çalışmaları başlatılmalıdır. Böylece birimlerin elindeki yıllardır birikmiş belgeler ayıklamaya tâbi tutularak, saklanması gereksiz olanların imhasına imkân sağlanmalı, Devlet Arşivleri'ne devredileceklerin devir işlemleri gerçekleştirilmeli, kurumunda saklanacakların daha sağlıklı ve güvenli ortamlarda muhafaza edilmeleri için gerekli şartlar oluşturulmalıdır.

Örneğin kişisel veri içeren Personel Özlük Dosyaları birim arşivinde "Emekli oluncaya kadar", kurum arşivinde ise "101 yıl doluncaya kadar" saklanmalıdır.
(http://www.akdenizbelbir.gov.tr/file.php?cat=1&file=42)

VERBİS kaydı her kamu kurum ve kuruluşunun veya şirketin kendine has faaliyetleri, kişisel veri toplama noktaları, işleme amaçları, paylaşımları gibi etkenlere özgü olarak yapılmalıdır. Bu kapsamda bir belediyenin **ÖRNEK VERBİS** kaydına bu adresten ulaşılabilmektedir: www.kocarslanhukuk.com/verbis.pdf

YAPTIRIMLAR

CEZA HÜKÜMLERİ

Kanunun 17. maddesinde kişisel verilere ilişkin suçlar bakımından 5237 Sayılı Türk Ceza Kanununun ilgili maddelerine atıfta bulunulurken, 18. maddesinde ise kabahat niteliğini haiz fiiller düzenleme altına alınmıştır.

Buna göre, kişisel verilerin işlenmesine ilişkin hukuka aykırılıkları suçlar ve kabahatler olarak iki başlık altında incelemek mümkündür.

Suçlar

Kanunun 17. maddesine göre; "(1) Kişisel verilere ilişkin suçlar bakımından 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140'ıncı madde hükümleri uygulanır. (2) Bu Kanunun 7'nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hale getirmeyenler Türk Ceza Kanununun 138'inci maddesine göre cezalandırılır."

Kişisel verilere ilişkin suçlar, TCK'nın "Özel Hayata ve Hayatın Gizli Alanına İlişkin Suçlar" bölümü içerisinde ele alınmıştır.

TCK'nın 135. maddesinin 1. fıkrasına göre: *"Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir"*. Kanunda ve TCK'nın ilgili madde gerekçesinde kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanan kişisel verilerin hukuka aykırı şekilde kaydedilmesi, suçun oluşması için yeterlidir. Burada suçun oluşumunun ön şartının hukuka aykırılık olarak belirlendiğine dikkat çekmek gerekir. TCK'nın 135. maddesinin 2. fıkrasına göre: *"Kişisel verilerin, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."*

TCK'nın 136. maddesine göre: *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır"*. TCK'nın 135. maddesindeki düzenlemeye benzer şekilde kişisel verilerin üçüncü bir kişiye verilmesi, yayılması ya da ele geçirilmesi suçlarının hukuka aykırılık ön şartına bağlandığı görülmektedir.

TCK'nın nitelikli hallerin düzenlendiği 137. maddesine göre: *"Yukarıdaki maddelerde tanımlanan suçların*;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır."

TCK'nın 138. maddesine göre: *"(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir. (2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."*

TCK'nın 139. maddesinde şikâyet usulü düzenlenmektedir. Buna göre, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır.

TCK'nın 140. maddesinde, yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı belirtilmektedir.

Kabahatler

Kanunun 18. maddesine göre: " (1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk Lirasından 100.000 Türk Lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk Lirasından 1.000.000 Türk Lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk Lirasından 1.000.000 Türk Lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk Lirasından 1.000.000 Türk Lirasına kadar,

idari para cezası verilir

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir."

Maddede aydınlatma, veri güvenliğini sağlama, Kurul kararlarını yerine getirme, Veri Sorumluları Siciline kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak düzenlenmiş ve Kurul tarafından belirlenecek idari para cezası yaptırımına bağlanmıştır.

İdari para cezaları, veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacaktır. **Maddede kabahat olarak düzenlenen eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacaktır.** İlgili kurumlar yaptıkları soruşturmanın sonuçları hakkında Kurula bilgilendirme yapmak zorundadır.

SONUÇ VE DEĞERLENDİRME

Kamu kurum ve kuruluşlarında, belediyelerde ilgili kişilere hizmet amaçlı olarak birçok kişisel veri işlenmektedir. Bu doğrultuda hangi kişisel verilerin hangi amaca hizmet etmek için işlendiği hususları ortaya konulmalı, kişisel veriler genel ilkelere uygun olarak işlenmeli, gerek olmayan kişisel verilerin imhası yapılarak kişisel veriler azaltılmalı, kişisel veri işleme envanteri hazırlanmalıdır. Bir şekilde kişisel veriyi ilgilendiren her türlü hukuki ilişki kurulan taraflarla olan sözleşmeler güncellenmeli, kurum içi gizlilik taahhütnameleri yapılmalı, ilgili kişiler aydınlatılmalı ve gerektiği durumlarda açık rızalar alınmalıdır. Kurum içinde idari tedbirler alınmalı ve bununla da yetinilmeyerek veri güvenliği sağlamak adına gerekli ve makul düzeyde teknik tedbirler de alınmalıdır. Teknik donanım tedbirleri ile de yetinilmeyip mutlaka siber güvenlik amaçlı sızma testi (penetrasyon testi) yapılmalı ve ortaya çıkan güvenlik zafiyetleri giderilmelidir. Bir başka deyişle öncelikli olarak kişisel verilerin hukuka aykırı olarak işlenmesi engellenmelidir.

Veri güvenliğinin sağlanması 6698 sayılı kanun açısından son derece önemli olup uygulamada alınan tedbirler çoğu zaman yeterli olmamaktadır. Güvenlik halkasının en kilit noktası olan insan faktörü de dikkate alınmalıdır. Birçok zaman sosyal mühendislik ve oltalama saldırıları ile kişisel veriler çalınmaktadır. Bu noktada kurum içi periyodik olarak veri güvenliğine ilişkin eğitimler verilmeli, siber güvenlik farkındalığı artırılmalı ve kişisel verilerin korunması amaçlı bilgilendirme toplantıları yapılmalıdır. Yine de her ihtimale karşı kişisel verilerin çalınması durumunda oluşacak maddi ve manevi zararları teminat altına alan “Siber Güvenlik Sigortası” yapılmalıdır.

Belediyeler veri sahibi olan vatandaşlarını veriye temas ettiği noktada aydınlatmalı, gerek görüldüğü takdirde kamu spotu, bilgilendirme afişleri, internet sitesi, yerel televizyon reklamları ile ilgili kişinin hakları bildirilmelidir. Kurumun veri yaşam döngüsüne uygun olarak kişisel veri işleme envanteri hazırlanmalı ve bununla paralel olarak son kayıt tarihine kadar VERBİS kaydı yapılmalıdır. Bütün bunlar yapılırken belediyelerin ilgili birimleri ve elzem olarak bilgi işlem ve hukuk birimleri birlikte çalışmalıdır. Kanunun uzmanlık gerektirmesinden dolayı yetersizlik halinde siber güvenlik ve hukuk danışmanlığı alanlarında uzman desteği alınmalıdır.