

ÇAĞRI MERKEZLERİ DERNEĞİ
KİŞİSEL VERİLERİN KORUNMASI KANUNU ÇALIŞTAYINA DAİR
SORULAR VE CEVAPLAR - 30/03/2017

1. Açık rıza nedir ve hangi yöntemle alınır?

Açık rıza, Kanunun 3/a maddesine göre, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür irade ile alınan rıza anlamına gelmektedir. Açık rıza her türlü iletişim aracı ile alınabilir. Burada dikkat edilmesi gereken husus; ticari elektronik iletiler için onay alınırken bu onay internet ortamında alınıyorsa, onay kutusunun önceden otomatik işaretlenmemiş olarak gelmesi eğer fiziki bir form ile onay alınıyorsa görünür ve okunaklı bir metin ile alınması gerekmektedir.

2. Adres değişikliği gibi bilgi güncelleme işlemleri de veri işleme kapsamında mıdır, müşteri talebi olarak değerlendirilebilir mi?

Evet, kanuna göre adres değişikliği de veri işleme olarak kabul edilir ve Kanun'un 11/d hükmü uyarınca veri sorumlusundan ilgili değişiklik talep edilebilir.

3. Kişisel verilerin yok edilmesi ya da anonim hale getirilmesine ilişkin prosedür nedir?

Kişisel verilerin yok edilmesi veya anonim hale getirilmesi hususu Kanun'un 7. Maddesi ile getirilen bir yükümlülük olup bu verilerin nasıl anonim hale getirileceği veyahut nasıl yok edileceğinin bir Yönetmelik ile düzenleneceği belirtilmiş ise de ilgili yönetmelik ne yazık ki henüz çıkarılamamıştır.

4. Kişisel verilerin aktarılması, yurt dışına aktarılmasına ilişkin prosedür nedir? Burada bahsi geçen yeterli önlemler nelerdir?

Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

Yurtdışına veri aktarımı için kanun birtakım şartlar aramıştır. Öncelikle verinin aktarılabilmesi için aşağıdaki şartların varlığı gerekecektir:

- ✓ Kanunlarda açıkça öngörülmesi,

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

Ve Aktarılacağı Ülkede,

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

5. Verilerin aktarılacağı ülkede verilerle ilgili yeterli korumanın olup olmadığına Kurul nasıl karar verecektir?

Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına;

- ✓ Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
- ✓ Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
- ✓ Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini,
- ✓ Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- ✓ Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,

değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

6. Yurtdışında yeterli korumanın bulunduğu ülkeler hangileridir?

Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilecek olup bu ülkeler hakkında açıklama yakın bir zamanda Veri Koruma Kurulu'na yapılacaktır.

7. Veri sorumlusu şahıs mıdır, şirketler midir? Şirketlerde bu tür bir pozisyon gerekli midir? Şirket içinde sorumlu kimdir?

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Ayrıca veri sorumlusunun Veri Sorumluları Sicil'ine de kaydolması gereklidir. Bu tanım uyarınca “gerçek kişi verisi” toplayan ve işleyen herkes veri sorumlusudur. Şirketler dilerlerse doğrudan kendileri veri sorumlusu konumunda olabilecekleri gibi bir pozisyon ile de veri sorumlusunu belirleyebilirler. Ancak bu yönde Veri Koruma Kurulu nezdinde bir sorumluluk doğduğunda ilgili ceza/tazminat öncelikle şirkete yönelik olacak, sorumlu personele yönelik şirketin rücu hakkı saklı olacaktır. Bunun yanında fiili işleyen gerçek kişinin de doğrudan cezai sorumluluğuna gidilebilecektir.

8. Veri sorumlusunun kendi kuruluşunda yapmakla yükümlü olduğu denetimin periyodu nedir, standardı var mıdır?

Veri sorumlusu her gün ve her dakika kişisel verilerin korunması için kendinden beklenebilecek önlemleri almakla ve bu önlemleri denetlemekle yükümlüdür. Daha açık bir ifade ile veri sorumlusunun en üst düzeyde sürekli bir kontrol ve denetim sağlaması gerekmektedir.

9. Çalışan tarafında teknik ve prosedürel her türlü önlem alınmış olmasına rağmen, manuel yollardan bilgilerin ele geçirilmesi halinde sorumluluk çalışanda mı yoksa şirkette mi olacaktır?

Kanunun 12. Maddesine göre işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirmekle yükümlü olup sorumluluk öncelikle veri sorumlusunda olacaktır. Veri sorumlusu ise ilgili ceza ve tazminatları ödedikten sonra ceza hukukuna ve özel hukuka dair haklarını çalışanına rücu etme hakkına sahip olacaktır.

10. Dış kaynak çağrı merkezleri isim veya numara gibi kişisel bilgilerin bir kısmının görüneceği bir şekilde müşteri ile sözleşme yapması halinde dış kaynak şirket sorumluluktan muaf olabilir mi?

Kanunun 8. Maddesinin atfı ile 5/2-c hükmü uyarınca; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde verilerin işlenmesi ve aktarılması mümkün olup dış kaynak şirket sorumluluktan muaf olabilir. Ancak bu durum olabildiğince dar yorumlanmalıdır. Olası veri ihlallerinde asli sorumluluk her zaman veri sorumlusu şirkette olacak, ancak veri işleyen sıfatını haiz olan dış kaynak çağrı merkezleri de, işledikleri verinin güvenli olarak saklanmasından ve yetkisiz kişilerce erişiminin engellenmesinden sorumlu olacaklardır.

11. Çalışanların kişisel bilgilerinin işyeri tarafından işlenecek, kullanılacak olması halinde kişiden onay almak gerekli midir? (Ör, iş başvuruları vb.)

Kanunun 3/1-e hükmünde 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 işlem olarak tanımlandığı için kişilerinin onayları alınmadan işlenmesi mümkün değildir. Burada dikkat edilmesi gereken bir diğer husus ise Kanunun 6. Madde uyarınca, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veriler olup özel nitelikli kişisel verilerin, ilgilinin *açık rızası olmaksızın* işlenmesi yasaktır.

12. Veri sorumlusu siciline şirketler mi yoksa şahıslar mı kayıt olacaktır? Veri sorumluları siciline ilişkin prosedürler nelerdir?

Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Bu kayıt Kişisel Verileri Koruma Kurumu Başkanlığı'na Kanunun 16/3. Hükmünde yer alan belgelerle yapılır. Prosedürün yönetmelik ile düzenleneceği belirtilmiş olup henüz daha yönetmelik yürürlüğe girmemiştir.

13. İdari para cezalarının miktarı ne şekilde belirlenmektedir? Ceza öncesi bir ihtar mekanizması mevcut mudur?

İdari para cezalarına kaynak olan şikayetler için bir prosedür söz konusu olmasına rağmen herhangi bir ihtar mekanizması bulunmamakta doğrudan ceza uygulanmasına gitmektedir.

Kanunun 18. Maddesin belirtilen idari para cezaları ise şu şekildedir:

Bu Kanunun;

- ✓ 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
 - ✓ 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
 - ✓ 5 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
 - ✓ 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.

Hemen belirtelim ki bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

14. Kanuna ilişkin tebliğleri ve uygulama esasları kim tarafından çıkarılacaktır?

Kanuna ilişkin tebliğ ve yönetmelikler Veri Koruma Kurumu tarafından çıkarılacaktır.

15. Diğer ülkelerdeki uygulama modelleri nelerdir?

- ✓ ABD’de liberal opt-out sistemi ancak ağır cezalar; FTC kontrolü, Finans, Telekom, Sağlık ve Çocuklara yönelik özel düzenlemeler / hassas kişisel veriler için izin gerektiren halleri içeren düzenlemeler mevcuttur.
- ✓ AB’de opt-in sistemi; AB Mevzuatın çerçevesinde sıkı denetim mevcut olup ülkemizde de bu sistem kullanılmaktadır.
- ✓ Uzakdoğu’ya baktığımız zaman ise ABD ve AB modellerinin ülkeden ülkeye değişiklik göstererek birlikte uygulandığını görüyoruz.

16. Kanun henüz yürürlüğe girmeden önce, imzasınız formlarda bulunan veriler kaydedilip, Kanun yürürlüğe girdikten sonra veri kayıtlarının silinmemesi üzerine yaptırım nedir?

- ✓ Kanun'un yürürlük başlıklı 32. Maddesine göre; Kanunun 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra,
- ✓ Diğer maddeleri ise yayımı tarihinde, yürürlüğe girecektir.

Kanun'un 07.04.2016 tarihinde yayınlandığı dikkate alındığında Kanunun tüm maddelerinin yürürlüğe girdiğini söylemek yanlış olmayacaktır. O halde bu bilgiler Kanuna aykırı olarak edinilmiş bilgiler olup ilgili veriler için veri sahibinden izin alınmaması halinde silinmesi veya anonim hale getirilmesi şarttır. Ancak, Ticari İletişim ve Ticari Elektronik İletiler Hakkında mevzuat hükümleri saklıdır.

17. Kanun henüz yürürlüğe girmeden önce, imzasınız formlarda alınıp kaydedilen veriler için Kanun yürürlüğe girdikten sonra veri kayıtlarının kullanımı hakkında Ticari İletişim ve Ticari Elektronik İletiler Hakkındaki saklı mevzuat hükümleri nelerdir?

< 1 Mayıs 2015 (E – ticaret Kanunu) Öncesi	1 Mayıs 2015 Sonrası > (E-ticaret Kanunu)	15 Temmuz 2015 Sonrası > (Ticari İleti Yönetmeliği)	7 Nisan 2016 Sonrası > (Kişisel Veriler Kanunu)
İstisnalar; ticari ileti gönderilmesi amacıyla alınmış herhangi bir şekilde onay + mal ve hizmet teminine yönelik işlemler sırasında alınan iletişim bilgisi	Ana Kural: Önceden yazılı (fiziki ya da sanal ortamda) onay şartı. İstisnası; < 1 Mayıs kurallarına uygun toplanan veriler	Ana Kural: Ayrı bir metin ile alınmış açık izin (opt-in). İstisnası; 15 Temmuz ve 1 Mayıs'tan önce toplanmış veriler; 1 Mayıs öncesi istisnalarına tabi	Ana Kural: Kanuna uygun olarak genişletilmiş şekilde açık rıza ile alınmış izin. İstisnası: 7 Nisan öncesi dönemde hukuka uygun uygun alınmış izinler; 1 Mayıs istisna kuralları

18. Veri sorumlusu ve veri işleyen arasındaki rücu ilişkisi ve 3. Kişilere karşı sorumluluk gözetilerek, Kanunun 12. Maddesinde düzenlenen veri sorumlusu ve veri işleyenin müşterek sorumluluğu husus nasıl değerlendirilmelidir?

Kanun sistematığıne baktığımızda veri sahibine karşı asli sorumlu her zaman veri sorumlusudur. Ancak yine Kanun'nun uygun gördüğü şekilde verinin işlenmesine yönelik bazı yetkilerini, bir sözleşme ilişkisiyle, bir 3.kişiye devredebilir. Buradaki sorumluluk her

ne kadar birlikte sorumluluk anlamına gelmekte ve veri işleyenlere karşı da sorumluluğa gidilebileceği yönünde lafzi yoruma gidilebilecek olsa da, Kanun koyucunun buradaki asıl amacının, veri sorumlusunun asli sorumluluğunu, veri işleyene yetki devri halinde de korumak olduğunu düşünmekteyiz.

19. Aydınlatma Yükümlülüğünün Kapsam ve Usulü nedir ?

Kanunun 10. Maddesi veri sorumlusunun aydınlatma yükümlülüğünü şu şekilde düzenlemiştir:

Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

- a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
 - b) Kişisel verilerin hangi amaçla işleneceği,
 - c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
 - ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
 - d) 11 inci maddede sayılan diğer hakları,
- konusunda bilgi vermekle yükümlüdür.

Aydınlatma her türlü iletişim aracıyla yapılabilir. Ancak veri sahibinin yazılı başvurusu üzerine en kısa sürede veya en geç 30 gün içinde yerine getirmekle yükümlüdür.

20. Uygulamada veri sorumlusu şirketler, outsource işlerde veri işleyen şirketlere sözleşme ile her türlü idari yaptırımı devretme gayreti içindedirler. Kanun ve uygulamada sorumluluğun sınırı belirlenmesi konusunda değerlendirme nasıl olmalıdır?

Kanunun 12/2. hükmüne göre veri sorumlusunun her halde veri işleyen ile birlikte ve hatta aslen sorumludur. Bu sebeple kanunun bu emredici hükmüne karşı bir anlaşma ile bu durumun aksinin kararlaştırılması mümkün gözükmemektedir.

21. Veri sorumlusu kişi veya kurumların kişisel verileri korumak amacıyla güvenlik düzeyini temin etmek amacıyla her türlü teknik ve idari tedbiri almaları gerekmektedir. Buradaki “her türlü teknik ve idari tedbir” teriminden ne anlamak gerekmektedir?

Bu terimin sınırları Kanunda açıkça belirtilmemiş olmakla beraber bu sorumluluğun bir “kusursuz sorumluluk” olduğundan bahsedebiliriz. Buna göre, verilerin güvenliğinin sağlanması amacıyla veri sorumlusu her türlü teknik ve idari almakla yükümlü olup sorumluluğunun doğması için kusurunun bulunması aranmayacaktır. Bir diğer ifade ile verilerin güvenliği bir kusur sebebiyle tehlikeye düşmemiş olsa bile veri sorumlusu sorumluluktan kurtulamayacaktır.

Buna ek olarak Őirket veya tacirlerin veri sorumlusu konumunda olmaları halinde bu sorumluluĐa bir de Trk Ticaret Kanunu'ndaki 18/2 hkm uyarınca bir tacir btn ticaretine ait btn faaliyetlerinde basiretli bir iŐ adamı gibi hareket etmesi gerekmektedir. Bu kavram ise tacire, objektif bir zen lt getirmektedir. Tacirler faaliyetlerinde tedbirli ve tecrbeli bir iŐ adamı gibi davranmak zorundadır.

*** Bu alıŐma, Av.Emre Berk tarafından hazırlanmıŐ olup, yalnızca ÇaĐrı Merkezleri DerneĐi alıŐtayını kapsamında genel bir bilgilendirme notu niteliĐindedir. Daha detaylı ihtiyalarınıza ynelik kurumunuza zel danıŐmanlık hizmeti almanızı neririz.**