

## DENET SİRKÜLER

Yönetişim, Risk ve Uyum

**BDO**

AUDIT | TAX | ADVISORY

For the latest from BDO Turkey, follow us



**Sirküler Tarihi : 14.04.2025**  
**Sirküler No : 2025/001**

### 7545 SAYILI SİBER GÜVENLİK KANUNA: TÜRKİYE’NİN SİBER UZAYDAKİ MİLLİ GÜCÜNÜ GÜÇLENDİRME HAMLESİ

#### İçindekiler

|                                                                                                      |   |
|------------------------------------------------------------------------------------------------------|---|
| 7545 Sayılı Siber Güvenlik Kanunu: Türkiye'nin Siber Uzaydaki Millî Gücünü Güçlendirme Hamlesi ..... | 1 |
| Giriş .....                                                                                          | 2 |
| Kanunun Temel Amaçları ve Kapsamı.....                                                               | 2 |
| Kilit Tanımlar ve Temel İlkeler.....                                                                 | 2 |
| Kurumsal Yapı ve Görevler.....                                                                       | 3 |
| Personel, Gelir ve Muafiyetler.....                                                                  | 4 |
| Denetimler ve Cezai Hükümler.....                                                                    | 4 |
| Siber Güvenlik Ürünleri ve Hizmetleri.....                                                           | 5 |

#### **BDO Yayıncılık A.Ş.**

Eski Büyükdere Cad. No.14  
Park Plaza Kat:4  
34398 Maslak/İstanbul  
Turkey

Tel: +90 212 365 62 00  
Fax: +90 212 365 62 02  
e-mail: bdo@bdo.com.tr  
[www.bdo.com.tr](http://www.bdo.com.tr)

*Garantisi ile sınırlı bir Birleşik Krallık şirketi olan BDO International Limited'in üyesi ve bir Türk anonim şirketi olan BDO Yayıncılık A.Ş., bağımsız üye kuruluşlardan oluşan BDO ağıının bir parçasını teşkil etmektedir.*

*BDO International global ağıının toplam gelirleri 2024 yılında 15 milyar ABD Doları olarak gerçekleşmiştir. BDO, 166'dan fazla ülkede bulunan 1.800 ofiste faaliyet göstermekte olup, bu ofislerde denetim ve danışmanlık hizmetleri veren ortaklar dahil dünya çapında 119.611 kişi çalışmaktadır.*

*Dikkat ve titizlikle hazırlanan bu yayın, geniş anlamda görüşleri içermekte olup, genel bir yol gösterici olarak değerlendirilmelidir. Özel durumlarla ilgili olarak, mesleki görüş ve yardım almadan, bu yayına dayanarak uygulamalarda bulunulmamalıdır. Bu konuların kendi özel durumunuza ilişkin etkilerini görüşmek için BDO Yayıncılık A.Ş. ile temas kurabilirsiniz. Bu yayındaki bilgilere dayanarak belli eylemlerde bulunmak veya bulunmamak nedeniyle doğabilecek zararlar nedeniyle, BDO Yayıncılık A.Ş. ve ortakları, çalışanları ile yazarları herhangi bir yükümlülük veya sorumluluk kabul etmemektedirler.*

## Giriş

Türkiye, siber uzaydaki milli güvenliğini sağlamak ve dijital varlıklarını korumak amacıyla kapsamlı bir yasal düzenlemeyi yürürlüğe koydu. Yeni Siber Güvenlik Kanunu (Kanun), Türkiye'nin siber uzaydaki milli gücünü korumak ve sürdürülebilir bir dijital güvenlik mimarisi inşa etmek için yasal ve kurumsal düzenlemeler getirmektedir. Ülkenin siber güvenliğini tehdit eden iç ve dış kaynaklı mevcut ve muhtemel tehlikelerin tespiti ve bertaraf edilmesi, siber olayların etkilerinin en aza indirilmesi, kamu kurum ve kuruluşları başta olmak üzere tüm ilgili aktörlerin siber saldırılara karşı korunmasına yönelik temel esasları ve stratejileri belirlemektedir. Türkiye'nin siber güvenliğini güçlendirmek amacıyla atılmış stratejik bir adım olarak öne çıkan bu yasa, siber güvenlik alanında merkezi otoriteyi tanımlamaktadır. Aynı zamanda kamu ve özel sektörün yanı sıra gerçek kişileri kapsayan geniş bir alanda siber güvenlik stratejilerinin uygulanmasını zorunlu kılmakta, düzenlemelere aykırı tutum ve davranışlar ile ilgili cezai yaptırımları tanımlamaktadır.

## Kanunun Temel Amaçları ve Kapsamı

Siber Güvenlik Kanunu'nun temel amacı, Türkiye Cumhuriyeti'nin siber uzaydaki varlıklarını iç ve dış tehditlerden korumak, kritik altyapıların dayanıklılığını artırmak ve ulusal çapta siber güvenlik stratejilerini belirlemektir. Bu doğrultuda kanun, siber olayların muhtemel etkilerini azaltmayı, kamu ve özel sektörün siber saldırılara karşı korunmasını sağlamayı ve ülkenin genel siber güvenlik seviyesini yükseltmeyi hedeflemektedir.

Kanunun kapsamı oldukça geniştir. Siber uzayda varlık gösteren, faaliyet yürüten veya hizmet sunan tüm kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlar bu kanun hükümlerine tabidir. Ancak, istihbari faaliyetler ile Türk Silahlı Kuvvetleri'nin iç hizmet kanunu kapsamındaki faaliyetler kanun kapsamı dışında tutulmuştur.

## Kilit Tanımlar ve Temel İlkeler

Kanun, siber güvenlik alanındaki temel kavramları net bir şekilde tanımlayarak uygulamada birliği sağlamayı amaçlamaktadır. "Siber uzay", "siber güvenlik", "siber saldırı", "siber tehdit", "kritik altyapı" ve "SOME" gibi önemli terimler detaylı bir şekilde açıklanmıştır.

Siber güvenliğin sağlanmasında benimsenen temel ilkeler ise şunlardır:

- Siber güvenlik milli güvenliğin ayrılmaz bir parçasıdır.
- Kritik altyapıların korunması ve güvenli bir siber uzayın oluşturulması temel hedeftir.
- Siber güvenlik çalışmaları kurumsal, sürekli ve sürdürülebilir bir yaklaşımla yürütülür.
- Siber güvenlik tedbirleri, hizmet ve ürünlerin tüm yaşam döngüsü boyunca uygulanır.

- Siber güvenlik çalışmalarında öncelikle yerli ve milli ürünler tercih edilir.
- Siber güvenlik politika ve stratejilerinin uygulanmasından tüm ilgili aktörler sorumludur.
- Siber güvenlik süreçlerinde hesap verebilirlik esastır.
- Siber güvenlik alanında nitelikli insan kaynağının geliştirilmesi teşvik edilir.
- Siber güvenlik kültürünün toplum geneline yaygınlaştırılması hedeflenir.
- Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması temel esaslardır.

### Kurumsal Yapı ve Görevler

Yeni yasayla birlikte **Siber Güvenlik Başkanlığı (Başkanlık)** ve **Siber Güvenlik Kurulu** adlı iki temel yapı kurulmuştur:

- **Siber Güvenlik Başkanlığı**, ülkenin siber güvenliğinin sağlanması ve koordinasyonundan sorumlu merkezi bir otorite olarak tanımlanmıştır. Ulusal siber güvenlik politikalarının belirlenmesi, uygulanması ve denetimi ile yetkilidir. Başkanlığın temel görevleri arasında şu başlıklar yer almaktadır
- Kritik altyapıların tespiti,
- Siber tehdit istihbaratının toplanması,
- SOME'lerin kurulması ve denetimi,
- Siber güvenlik standartlarını belirlenmesi,
- Siber güvenlik ürün ve hizmetlerinin test ve sertifikasyon süreçlerinin yürütülmesi.

**Başkanlığa verilen yetkiler oldukça kapsamlıdır.** İlgili kurum ve kuruluşlardan bilgi ve belge talep etme, siber olaylara müdahale etme, siber güvenlik denetimleri gerçekleştirme ve gerektiğinde yaptırım uygulama yetkileri bulunmaktadır. Bilişim sistemlerine müdahale, verilerin analiz edilmesi, log kayıtlarının toplanması, olaylara yerinde müdahale, kişisel verilerin işlenmesi gibi teknik ve hukuki işlemleri gerçekleştirme yetkisi mevcuttur.

Ayrıca, uluslararası kuruluşlar ve ülkelerle iş birliği yapma ve bilgi alışverişinde bulunma yetkisi de Başkanlığa tanınmıştır.

Kanun, siber uzayda faaliyet gösteren tüm aktörlere de önemli sorumluluklar yüklemektedir. Tüm kamu ve özel kuruluşlara, Başkanlıkla iş birliği yapma ve gerekli tedbirleri alma yükümlülüğü getirilmiştir. İlgili taraflar, Başkanlığın taleplerini zamanında iletmek, tespit ettikleri zafiyet ve siber olayları gecikmeksizin Başkanlığa bildirmekle yükümlüdür.

Özellikle kritik altyapılarda çalışan firmalar için Başkanlık tarafından yetkilendirilmiş ürün ve hizmet sağlayıcıları kullanma zorunluluğu vardır. **Siber Güvenlik Kurulu** ise ülkenin siber güvenlik politika ve stratejilerini belirlemek üzere üst düzey bir karar alma mekanizması olarak oluşturulmuştur. Kurul, Cumhurbaşkanı veya Cumhurbaşkanı Yardımcısı başkanlığında, ilgili bakanlar, Milli Güvenlik Kurulu Genel Sekreteri, Milli İstihbarat Teşkilatı Başkanı, Savunma Sanayii Başkanı ve Siber Güvenlik Başkanından oluşmaktadır.

Kurulun temel görevleri arasında şunlar yer almaktadır:

- Siber güvenlikle ilgili politika, strateji ve eylem planlarına yönelik kararlar almak,
- Kritik altyapı sektörlerini belirlemek,
- Siber güvenlik alanında teşvik edilecek öncelikli alanları saptamak,
- Başkanlık ile diğer kamu kurumları arasındaki ihtilafları çözmek.

### **Personel, Gelir ve Muafiyetler**

Kanun, Başkanlık bünyesinde siber güvenlik alanında uzmanlaşmış sözleşmeli personel istihdamına olanak tanımaktadır. Bu personelin nitelikleri ve ücretleri Siber Güvenlik Kurulu tarafından belirlenecektir. Ayrıca, Başkanlık personelinin güvenlik soruşturması ve arşiv araştırmasından geçirilmesi zorunlu kılınmıştır. Personel gizlilik yükümlülüğü altındadır; edindiği bilgi ve belgeleri yetkisiz kişilere açıklaması cezai yaptırıma tabidir. Görevden ayrılanlar için sektöre geçişte iki yıl boyunca kısıtlama uygulanacaktır. Başkanlığın gelir kaynakları arasında genel bütçe yardımları, faaliyetlerinden elde edilen gelirler, idari para cezaları ve Cumhurbaşkanı kararıyla fonlardan aktarılabilecek tutarlar yer almaktadır.

Başkanlığın ihtiyaçları kapsamında yapılacak ithalat ve hibe işlemleri gümrük vergisi, fon ve harçlardan muaf tutulmuştur.

Başkanlığın görevlerini yerine getirirken ihtiyaç duyduğu her türlü malzeme, araç, gereç, makine, cihaz ve sistemlerin ithalatı ve yurt dışına çıkışı için diğer kamu kurum ve kuruluşlarından veya özel sektörden izin ve uygunluk belgesi almasına gerek yoktur.

Ayrıca, kamu kurum ve kuruluşları ellerinde bulunan ve Başkanlığın görevleri için ihtiyaç duyulan her türlü malzeme, ekipman ve cihazı diğer yasal düzenlemelere bakılmaksızın Başkanlığa geçici olarak tahsis edebilir veya bedelsiz olarak devredebilirler.

### **Denetimler ve Cezai Hükümler**

Başkanlık, ilgili kurum ve şirketleri denetleyebilir, gerektiğinde mahallinde inceleme yapabilir. Denetim süreçlerine katılım zorunlu olup, gerekli bilgi ve belgelerin sağlanmaması durumunda ciddi yaptırımlar öngörülmektedir. Yetkilendirilen mercilere bilgi vermeyenler, gerekli onayları almadan faaliyet yürütenler, sır saklama yükümlülüğünü ihlal edenler, veri sızıntısına neden olanlar ve siber saldırı gerçekleştirenler hakkında hapis cezaları öngörülmektedir. Suçun kamu görevlisi, örgüt ya da birden fazla kişi tarafından işlenmesi halinde cezalar artırılabilmektedir.

Ayrıca, kanunda belirtilen görev ve sorumlulukları yerine getirmeyenlere yüksek miktarlarda idari para cezaları uygulanabilecektir. İdari para cezalarının uygulanmasında savunma hakkı tanınmakta ve cezaların tahsili Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre yapılmaktadır.

### **Siber Güvenlik Ürünleri ve Hizmetleri**

Yeni yasa, Türkiye’de geliştirilen veya faaliyette bulunan siber güvenlik ürünleri, sistemleri, yazılımları, donanımları ve hizmetlerinin satışı ve mülkiyet yapısındaki değişiklikleri sıkı kurallara bağlamaktadır. Siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerinin yurt dışına satışı, Siber Güvenlik Başkanlığı’nın belirlediği usul ve esaslara uygun şekilde yapılacaktır. İzne tabi ürünlerin satışı için Başkanlık onayı zorunludur.

Ayrıca, siber güvenlik şirketlerinin birleşme, bölünme ve devir işlemleri Başkanlığa bildirilecek ve kontrol hakkı değişiklikleri Başkanlık onayına tabi olacaktır.

Bu düzenlemeler ile amaç, siber güvenlik sektörünün sıkı bir şekilde denetlenmesini ve kontrol altında tutulmasını sağlamak, ürün ve teknolojilerin kontrolsüz el değiştirmesini engellemek ve dışa bağımlılığı azaltmaktır. Stratejik öneme sahip bu alandaki faaliyetleri düzenleyerek milli güvenlik çıkarlarını korumak hedeflenmektedir.