

# LBF Partners

---

## SİBER GÜVENLİKTE ÖNEMLİ ADIMLAR

### 7545 Sayılı Siber Güvenlik Kanunu Yürürlüğe Girdi

## SİBER GÜVENLİKTE ÖNEMLİ ADIMLAR 7545 Sayılı Siber Güvenlik Kanunu Yürürlüğe Girdi

### A. Giriş

Siber tehditlerin bertaraf edilmesi ve siber olayların muhtemel etkilerinin azaltılması amacıyla düzenlenen 7545 Sayılı Siber Güvenlik Kanunu (“Kanun”) 19.03.2025 tarihli ve 32846 sayılı Resmî Gazete’de yayımlanarak yürürlüğe girmiştir.

### B. Kanun ile Getirilen Önemli Düzenlemeler

Kanunun amacı Türkiye’nin siber güvenliğini sağlamak için iç ve dış tehditleri tespit ederek siber olayların etkilerini azaltacak esasları belirlemenin yanı sıra, kamu ve özel sektörün siber saldırılara karşı korunmasını sağlamak üzere genel esasların belirlenmesi olarak özetlenebilir.

Kanun kapsamına hem kamu tüzel kişileri hem özel tüzel kişiler hem de gerçek kişiler dahil edilmiş, istihbari faaliyetler ise istisna sayılmıştır.

#### 1. Siber Güvenlik Başkanlığı

Siber güvenliğin milli güvenliğin ayrılmaz bir parçası olması ilkesinden hareket eden Kanunda, siber güvenliğin sağlanması bakımından Siber Güvenlik Başkanlığına (“Başkanlık”) çeşitli görevler yüklenmiş olup, bu görevler arasından öne çıkanlar aşağıdaki gibidir:

- İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara ve güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar anlamına gelen kritik altyapılar ve

bilişim sistemlerinin siber saldırılara karşı korunmasına, siber saldırıların önlenmesine ve etkilerinin azaltılmasına yönelik faaliyet yürütmek,

- Kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek,
- Kamu kurumlarının ve kritik altyapıların siber güvenliğini sağlamak için gerekli altyapıları kurmak/kurdurmak, işletmek/ işlettirmek,
- Kamu kurum ve kuruluşlarına güvenli sistem ve altyapılar üzerinden barındırma hizmeti sunmak/sunulmasını sağlamak,
- Siber Olaylara Müdahale Ekipleri (SOME) kurmak, kurdurmak, denetlemek ve tatbikatlar ile müdahale kabiliyetlerini artırmak,
- Siber güvenlik alanında standartlar oluşturmak ve test ve sertifikasyon işlemleri yürütmek.

Başkanlık, Kanun kapsamında kendisine verilen görevleri yerine getirirken aşağıdaki iş ve işlemleri yapmaya da yetkili kılınmıştır:

- Kanun kapsamındaki kurumların siber saldırılardan korunmasını sağlamak amacıyla saldırılara karşı önleyici tedbirler almak/aldırmak,
- Siber saldırıya uğrayanlara yerinde veya uzaktan müdahale desteği sağlamak, saldırı izlerini takip etmek, delil oluşturmak ve suç şüphesi durumunda yetkililerle paylaşarak yerel ve uluslararası koordinasyonu sağlamak,

- Faaliyetle ilgili bilgi, belge ve verileri almak, değerlendirmek ve en fazla iki yıl süreyle kullanmak, sonra imha etmek,
- Bilişim sistemlerindeki log kayıtlarını toplamak, saklamak, değerlendirmek ve rapor hazırlayarak ilgili mercilerle paylaşmak.

Kanun'da ek olarak Başkanlığın yetkilerinin uygulanmasına ilişkin usul ve esasların çıkarılacak yönetmelikle belirleneceği düzenlenmektedir.

## 2. Görev ve Sorumluluklar

Kanun'da bilişim sistemleri kullanmak suretiyle hizmet sunan, veri toplayan, işleyen ve benzeri faaliyet yürütenlerin siber güvenliğe ilişkin görev ve sorumlulukları düzenlenmiş olup, bu sorumluluklar arasından öne çıkanlar aşağıdaki gibidir:

- Başkanlığın görev ve faaliyetleri kapsamında talep ettiği her türlü veri, bilgi, belge, donanım, yazılım ve diğer her türlü katkıyı öncelikle ve zamanında Başkanlığa iletmek.
- Hizmet sundukları alanda tespit ettikleri siber olayları veya siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından istismar edilebilecek zayıflık ve güvenlik açıklarını ifade eden zafiyetleri Başkanlığa bildirmek,
- Kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanlarından, üreticilerden veya şirketlerden tedarik etmek,
- Sertifikasyon, yetkilendirme ve belgelendirmeye tabi siber güvenlik şirketlerince faaliyete başlamadan önce

mevcut düzenlemeler çerçevesinde Başkanlığın onayını almak.

- Siber olgunluğun artırılmasına yönelik Başkanlık tarafından geliştirilen politika, strateji, eylem planı ile yayımlanan diğer düzenleyici işlemlerde yer alan hususları yerine getirmek ve gerekli tedbirleri almak.

## 3. Denetim

Kanun ayrıca Başkanlığı, Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş bağımsız denetçiler ve bağımsız denetim kuruluşlarını Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilerin Kanun hükümleriyle ilgili faaliyet ve işlemlerini denetlemek üzere yetkilendirmiştir.

## 4. Siber Güvenlik Kurulu

Kanun ile birlikte Siber Güvenlik Kurulu ("**Kurul**") da kurulmuştur. Cumhurbaşkanının başkanlık ettiği Kurul toplantılarına gündemin özelliğine göre üyeler dışından kişiler de çağrılıp bilgi ve görüş alınabilecektir.

Kurulun görevleri aşağıdaki gibidir:

- Siber güvenlikle ilgili politika vb. düzenleyici işlemlere yönelik kararlar almak,
- Teknoloji yol haritasının ülke çapında uygulanmasına yönelik karar almak,
- Siber güvenlik alanında teşvik verilecek öncelikli alanları belirlemek,
- Kritik altyapı sektörlerini belirlemek,
- Başkanlık ile kamu kurumları arasında meydana gelebilecek ihtilaflar hakkında karar almaktır.

## 5. Yaptırımlar

Kanun'un etkinliğinin artırılması ve caydırıcılığının sağlanması hedefiyle Kanun kapsamında getirilen yükümlülükler aykırı davranışlara yönelik olarak cezai hükümler ve adli para cezaları ayrıntılı olarak düzenlenmiştir:

- Kamu kurum ve kuruluşları hariç olmak üzere Kanun ile yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı vermeyenler veya bunların alınmasına engel olanlar bir yıldan üç yıla kadar hapis ve beş yüz günden bin beş yüz güne kadar adli para cezası ile cezalandırılır.
- Kanun uyarınca alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütenler iki yıldan dört yıla kadar hapis ve bin günden iki bin güne kadar adli para cezası ile cezalandırılır.
- Sır saklama yükümlülüğünü yerine getirmeyenlere dört yıldan sekiz yıla kadar hapis cezası verilir.
- Siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri, kişilerin veya kurumların izni olmaksızın ücretli veya ücretsiz şekilde erişime açan, paylaşan veya satışa çıkaranlara üç yıldan beş yıla kadar hapis cezası verilir.
- Siber uzayda veri sızıntısı olmadığını bildiği halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek amacıyla siber güvenlikle ilgili veri sızıntısı olduğuna yönelik gerçeğe aykırı içerik oluşturanlara veya bu maksatla bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir.
- Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik olarak siber saldırıda bulunan veya bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda bulunduranlara fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde sekiz yıldan on iki yıla kadar hapis cezası verilir. Bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda yayan, başka bir yere gönderen veya satışa çıkaranlara on yıldan on beş yıla kadar hapis cezası verilir.
- Kanun'dan kaynaklanan görev ve yetkilerini kötüye kullananlara veya kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet verenlere bir yıldan üç yıla kadar hapis cezası verilir.
- Bilişim sistemlerini kullanarak hizmet sunan, veri toplayan ve işleyenlerin; güvenlik açıklarını ve siber olayları Başkanlık'a bildirme yükümlülüğünü yerine getirmemeleri veya kamu kurum ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri, yetkili/sertifikalı siber güvenlik uzmanlarından ve şirketlerinden tedarik etmemeleri hâlinde bir milyon Türk lirasından on milyon Türk lirasına kadar idari para cezası verilir.
- Siber güvenlik ürünlerinin veya hizmetlerinin yurt dışına satışında veya siber güvenlikle ilgili her türlü ürünü/hizmeti üreten şirketin birleşme, devir veya satış işlemlerinde Başkanlık'ın görüşüne veya onayına başvurulmaması veya Başkanlığın bilgi

edinme yazılarına cevap verilmemesi on milyon Türk lirasından yüz milyon Türk lirasına kadar idari para cezası verilir.

- Denetçiler ile iş birliği yükümlülüğünü yerine getirmeyenler hakkında yüz bin Türk lirasından bir milyon Türk lirasına kadar, bu yükümlülüklerin ticari şirketlerce yerine getirilmemesi halinde yüz bin Türk lirasından az olmamak üzere bağımsız denetimden geçmiş yıllık finansal tablolarında yer alan brüt satış hasılatının yüzde 5'ine kadar idari para cezası verilir.

## 6. Siber Güvenlik Ürünleri ve Şirketleri

Kanun, siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı, Başkanlıkça belirlenecek usul ve esaslara uygun olarak yapılacağını düzenlemiştir. Ek olarak siber güvenlik şirketlerinin pay sahipliğindeki değişiklikler de Başkanlık iznine tabi tutulmuştur.

## C. Sonuç

Kanun ile ulusal siber güvenliğin güçlendirilmesi amacıyla genel bir çerçeve çizilmiş ve hem kamuyu hem özel sektörü ilgilendiren düzenlemelerin temeli atılmıştır. Kanun kapsamına dahil gerçek ve tüzel kişilerin, özellikle önümüzdeki bir yıl içinde gerçekleştirilecek ikincil düzenlemeleri de takip ederek uyum faaliyetlerini yürütmesi gerekecektir.

Daha fazla bilgi ve destek için [info@lbpartners.com](mailto:info@lbpartners.com) adresinden bizimle iletişime geçebilirsiniz.

**LBF Partners Hukuk Bürosu**