

**YÖNETMELİK**

Bankacılık Düzenleme ve Denetleme Kurumundan:

**BANKA KARTLARI VE KREDİ KARTLARI HAKKINDA  
YÖNETMELİKTE DEĞİŞİKLİK YAPILMASINA  
DAİR YÖNETMELİK**

**MADDE 1** – 10/3/2007 tarihli ve 26458 sayılı Resmî Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmeliğin 3 üncü maddesi aşağıdaki şekilde değiştirilmiştir.

**“MADDE 3** – (1) Bu Yönetmelik, 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 4, 5, 6, 8, 9, 10, 12, 13, 14, 21, 23, 24, 25, 26, 27 ve 29 uncu maddelerine dayanılarak hazırlanmıştır.”

**MADDE 2** – Aynı Yönetmeliğin 4 üncü maddesi aşağıdaki şekilde değiştirilmiştir.

**“MADDE 4** – (1) Bu Yönetmelikte geçen;

a) Bellenim: Firmware olarak bilinen ve bir donanım içerisindeki programlanabilir bellek üzerinde bulunan, donanımın tüm özelliklerini kullanabilmesi için ihtiyaç duyduğu, güncellenebilir yazılımı,

b) Diğer kuruluşlar: Kredi kartı çıkarma yetkisini haiz banka dışında kalan kuruluşları,

c) Kanun: 5464 sayılı Banka Kartları ve Kredi Kartları Kanununu,

ç) Kartlara ilişkin hassas veri: Banka kartı veya kredi kartı üzerinde yer alan ve ele geçirilmesi durumunda finansal işlem gerçekleştirmede kullanılabilecek bilgi setini/setlerini, ve ayrıca kart hamili doğrulamada kullanılan ve gizli kalması gereken PIN bilgisini,

d) Kartlı sistem kuruluşu: Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşları,

e) Kart çıkaran kuruluş: Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşları,

f) Kart kuruluşu: Kartlı sistem kuruluşu, kart çıkaran kuruluş ve üye işyeri anlaşması yapan kuruluşları,

g) Kurucu: Bir kart kuruluşunun sermayesinin veya oy haklarının doğrudan veya dolaylı olarak yüzde on veya daha fazlasını teşkil eden paylar ile bu oranın altında olsa dahi yönetim kurullarına üye belirleme imtiyazı veren paylara sahip gerçek veya tüzel kişileri,

ğ) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

h) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ı) Mali kurumlar: Ana faaliyet konuları para ve sermaye piyasaları olan ve bu konularda kendi özel mevzuatı uyarınca alınan izin ve ruhsat ile faaliyet gösteren kurumları,

i) POS: Banka kartı veya kredi kartı üzerindeki bilgileri esas alarak her türlü mal ve hizmet alımı veya nakit ödeme belgesi düzenlenmesi işlemleri ile bu Yönetmelik hükümleri uyarınca nakit kullanımı kapsamında değerlendirilebileceği belirtilen işlemlerin gerçekleştirilmesinde kullanılan elektronik cihazı,

j) Üye işyeri anlaşması yapan kuruluş: Banka kartı veya kredi kartı kabulünü sağlamak amacıyla işyerleriyle anlaşma yapan bankaları ya da kuruluşları,

k) 3D Secure: İnternet ortamında banka kartı veya kredi kartı ile gerçekleştirilen işlemlerde ek güvenlik katmanı getiren, kartlı sistem kuruluşları tarafından onaylı protokolü, ifade eder.”

**MADDE 3** – Aynı Yönetmeliğe 27 nci maddeden sonra gelmek üzere aşağıdaki madde eklenmiştir.

**“Teknik altyapıya ilişkin hususlar**

**MADDE 27/A** – (1) Üye işyeri anlaşması yapan kuruluşlar, kartlı ödeme işlemlerinde kullanılacak POS'un, asgari olarak Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi (Payment Card Industry -PCI- Security Standards Council) tarafından yayımlanan POS PIN Giriş Cihazı Güvenlik Gereksinimleri (PIN Entry Device -PED- Security Requirements) standardının güncel versiyonunun gereklerini, kartlı sistem kuruluşlarının tanımlamış oldukları süre çerçevesinde yerine getirmesini sağlarlar.

(2) POS, sahip olduğu güvenlik mekanizmaları ile asgari olarak aşağıdaki fonksiyonları yerine getirir;

a) Üzerinde yer alan bellenimin ve üye işyeri anlaşması yapan kuruluşlara ait uygulamalar gibi her türlü yazılımın, üye işyeri anlaşması yapan kuruluş veya bunlar tarafından görevlendirilmiş kişi veya taraflar haricinde kişilerce ve yetkisiz olarak erişilmeye karşı korumalı olmasını sağlamak için gerekli önlemleri üzerinde bulundurur. Bu önlemler, POS'a uzaktan yazılım yükleme ve yazılım güncelleme faaliyetlerini de kapsar. POS, kaynağını veya bütünlüğünü onaylamadığı yazılımları işleme almadan siler. POS üzerindeki kriptografik anahtarlara ve bu anahtarları işleyen hassas fonksiyonlara erişim kimlik doğrulama kontrolleriyle sağlanır.

b) POS, işleme tabi tutulmakta olan kartlara ilişkin hassas verilere yetkisiz fiziki veya elektronik erişimi engeller.

(3) Üye işyeri anlaşması yapan kuruluşlar, belirleyecekleri bir periyot çerçevesinde, kullandıkları POS'lar üzerinde koşmakta olan yazılımlarını, amaca uygun olmak kaydıyla kendilerinin belirleyeceği bütünlük ve geçerlilik testine tabi tutarlar.

(4) Üye işyeri anlaşması yapan kuruluşlar POS üzerindeki kendilerine ait yazılımların yüklenmesine ve güncellenebilmesine ilişkin yazılı ve denetlenebilir bir süreç oluşturur, sürecin işleyişine ilişkin gerekli detayda dokümantasyon tutar, kendilerine ait yazılımlarda gizlenmiş, yetkilendirilmemiş veya yazılı olarak kayda alınmamış fonksiyonların POS'ta barındırılmadığına ilişkin güvence oluşturacak düzeyde belgelendirme yapar. POS üzerinde yer alan ve işletim sistemi, bellenim gibi POS'un temel işlevlerini yerine getiren yazılımlar için benzer yapının kurulması sorumluluğu, POS'un bir üye işyeri anlaşması yapan kuruluşa ait olması durumunda söz konusu kuruluşa, aksi durumlarda ise POS sahibi merci tarafından belirlenecek üye işyeri anlaşması yapan kuruluşa aittir.

(5) Üye işyerleri, banka kartları veya kredi kartlarının fiziksel olarak doğrudan kart hamili tarafından bir cihaz üzerinde kullanıldığı durumlar ve Kanununun 20 nci maddesi kapsamındaki işlemler hariç olmak üzere, kartın POS veya POS kullanımının mümkün olmadığı durumlarda harcama veya nakit ödeme belgesi düzenleyen mekanik cihazlar haricinde bir cihaz üzerinden herhangi bir işleme tabi tutulmamasını sağlayacak alt yapıyı tesis ederler. Üye işyerleri, POS'un üye işyeri anlaşması yapan kuruluş sistemleri ile bağlantısını sağlayan alt yapı üzerinde, kartlara ilişkin hassas veriyi tutan, işleyen veya kaydeden bir sistem kuramazlar. Üye işyeri anlaşması yapan kuruluşlar, POS'un kendi sistemleri ile veri iletişimde asgari seviyede Ödeme Kartı Endüstrisi Veri Güvenliği Standardının (Payment Card Industry -PCI- Data Security Standard -DSS-) şifrelemeye ilişkin hükümlerini dikkate alırlar. Üye işyeri anlaşması yapan kuruluşlar, bu fıkra hükümlerinin üye işyerleriyle yapacakları sözleşmelerde yer almasını ve uygulanmasını gözetmekle yükümlüdürler.

(6) POS üzerinde işleme tabi tutulan banka kartı veya kredi kartından okutulan verilerden, üye işyerinin ihtiyaç duyacağı minimum veri setine karşılık gelen bölümü, bu veri setinin yetkisiz kişilerce ele geçirilmesi durumunda gizlilik ihlaline veya haksız menfaat sağlanmasına sebebiyet verilmemesi hususları da göz önünde bulundurulmak kaydıyla POS'un dış bağlantı ara yüzleri üzerinden aktarılır. Aktarma işlemi, üye işyeri anlaşması yapan kuruluşların POS üzerinde yer alan yazılımları tarafından, taraflar arasında belirlenecek formatta ve şekilde yapılır.

(7) Üye işyeri anlaşması yapan kuruluşlar ve üye işyerleri, harcama ve alacak belgesi düzenleme imkânı olmayan, kart hamili tarafından başlatılan ve internet kullanılarak gerçekleştirilen işlemler için diğer önlemlerle birlikte 3DSecure kart hamili doğrulama teknolojisini içerecek şekilde kart kullanım alt yapısı tesis ederler. Bu fıkra kapsamında gerçekleştirilecek işlemlerde söz konusu altyapının kullanımının zorunlu tutulması, üye işyeri anlaşması yapan kuruluşların ve üye işyerlerinin tercihlerine bağlı olup, zorunlu tutulmadığı durumlarda kullanım kart hamilinin tercihine bağlıdır. Kart hamili dışında kalan Kanun kapsamındaki taraflar, bu fıkra ile getirilen yöntem hakkında kart hamillerini bilgilendirirler.

(8) Üye işyeri anlaşması yapan kuruluşlarca, güvenlik alt yapısının daha kolay tesisi, operasyonel zorlukların en aza indirilmesi, kaynakların verimli kullanımı gibi hususlar yanında, kullanılan POS'ların teknolojik olanakları, kapasiteleri ve kesintisiz hizmet verilmesi kriterlerine göre, taraflar arasında yapılacak sözleşme hükümleri saklı kalmak kaydıyla, aynı POS üzerinde maksimum sayıda üye işyeri anlaşması yapan kuruluş uygulamasının çalışmasını sağlayacak bir yapı oluşturulur.”

**MADDE 4** – Aynı Yönetmeliğin 29 uncu maddesi aşağıdaki şekilde değiştirilmiştir.

**“MADDE 29** – (1) Bu Yönetmeliğin;

a) 27/A maddesinin birinci fıkrası 1/1/2009, dördüncü, beşinci, altıncı ve sekizinci fıkraları 1/1/2010, üçüncü ve yedinci fıkraları 1/1/2011, ikinci fıkrası 1/1/2014 tarihinde,

b) Diğer maddeleri 1/3/2007 tarihinden itibaren geçerli olmak üzere yayımı tarihinde, yürürlüğe girer.”

**MADDE 5** – Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

**MADDE 6** – Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

<b>Yönetmeliğin Yayımlandığı Resmî Gazete'nin</b>	
<b>Tarihi</b>	<b>Sayısı</b>
10/3/2007	26458