TEBLİĞ

Türkiye Cumhuriyet Merkez Bankasından:

ÖDEME VE MENKUL KIYMET MUTABAKAT SİSTEMLERİNDE KULLANILAN BİLGİ SİSTEMLERİ HAKKINDA TEBLİĞ
(Sayı: 2015/7)

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Tebliğin amacı, ödeme ve menkul kıymet mutabakat sistemlerine ilişkin faaliyetlerin yürütülmesinde kullanılan bilgi sistemleri ile ilgili usul ve esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Bu Tebliğ, ödeme ve menkul kıymet mutabakat sistemlerine ilişkin faaliyetlerin yürütülmesinde kullanılan bilgi sistemleri ile ilgili olarak, bilgi sistemleri yönetimine ilişkin genel hükümlere, bilgi güvenliği yönetimine, güvenlik açıkları ve ihlallerine, denetim izlerine, kimlik doğrulama, erişim denetimi ve inkar edilemezliğe, bilgi sistemlerine ilişkin risk yönetimine, bilgi sistemleri işletimine, bilgi sistemleri süreklilik planına, bilgi sistemlerinde dış hizmet alımına ve diğer hususlara ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 – (1) Bu Tebliğ, 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun 4 üncü maddesinin üçüncü fıkrasına, 28/6/2014 tarih ve 29044 sayılı Resmî Gazete'de yayımlanan Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmeliğin 24 üncü maddesinin dokuzuncu fıkrasına ve 30 uncu maddesinin birinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu Tebliğde yer alan;

a) Banka: Türkiye Cumhuriyet Merkez Bankası Anonim Şirketini,

b) Bilgi sistemleri: Ödeme ve menkul kıymet mutabakat sistemlerine ilişkin faaliyetlerin yürütülmesi amacıyla sistem işleticilerinin bilgi ve verilerle ilgili olarak mevzuatla belirlenmiş sorumluluklarının yerine getirilmesini sağlayan donanım, yazılım, veri ve süreçlerden oluşan yapının tamamını,

c) Bilgi sistemleri süreklilik planı: Bilgi sistemlerinin kesintisiz işlemesini olumsuz etkileyebilecek, siber saldırıları da dikkate alan her türlü olağan dışı duruma ilişkin senaryolar ile bu senaryoların gerçekleşmesi halinde bilgi sistemlerinde yaşanabilecek kesintilerin makul bir süre içinde ve veri kaybı olmaksızın giderilmesine ilişkin hususları da içerecek planı,

ç) Bilgi sistemleri yönetimi: Ödeme ve menkul kıymet mutabakat sistemlerinin faaliyetlerinin kesintisiz, güvenli, etkin ve verimli bir şekilde yürütülmesi amacıyla uygun bilgi sistemlerinin tesis edilmesine, bilgi sistemleri kaynaklarının etkin ve verimli olarak kullanılmasına, bilgi güvenliği yönetimine, bilgi sistemlerine ilişkin risklerin yönetilmesine ve bilgi sistemlerinin sürekliliğinin sağlanmasına ilişkin faaliyetleri,

d) Değişiklik yönetimi: Önceden belirlenmiş prosedürlerin kullanımı yoluyla bilgi sistemleri ile ilgili tüm değişikliklerin etkin ve güvenli bir şekilde ve zamanında gerçekleştirilmesini sağlamayı ve bu değişikliklerden kaynaklanabilecek olayların sayısı ile bu olayların sunulan hizmetler üzerindeki etkisini asgari düzeye indirmeyi amaçlayan bilgi sistemleri hizmet yönetimi disiplinini,

e) Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,

f) Faaliyet Yönetmeliği: 28/6/2014 tarihli ve 29044 sayılı Resmî Gazete'de yayımlanan Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmeliği,

g) Hizmet seviyesi: Hizmetlerin maliyeti ile söz konusu hizmetleri alanların gereksinim ve beklentilerinin göz önünde bulundurulması suretiyle, sistem işleticisi tarafından hizmetlerin içeriği ve kalitesine ilişkin yazılı olarak önceden belirlenen ve ilgili taraflarla paylaşılan seviyeyi,

ğ) Kapasite yönetimi: Bilgi sistemlerinin mevcut kapasite ve performansının izlenmesini, stres testleri de dahil olmak üzere test edilmesini, iş ihtiyaçları ve teknik gereksinimler ile iş sürekliliği hedefleri doğrultusunda gözden geçirilerek planlanmasını içeren faaliyetleri,

h) Katılımcı: Sisteme katılarak doğrudan transfer emri verme yetkisi bulunan ve sistem kurallarına uymakla yükümlü tüzel kişiyi,

ı) Menkul kıymet mutabakat sistemi: Üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan menkul kıymet aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapıyı,

i) Olay: Bilgi sistemlerinin işleyişinde planlanmamış bir kesintiye ya da güvenlik ihlalleri dahil hizmet kalitesinde düşüşe neden olan her türlü gelişmeyi,

j) Ödeme sistemi: Üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapıyı,

k) Proje yönetimi: Önceden belirlenmiş metodolojilerin kullanımı yoluyla bilgi sistemleri projelerinin, öngörülen zaman planına, bütçeye ve kalite düzeyine uygun olarak tamamlanmasını temin edecek şekilde planlanmasını, organizasyonunu ve yürütülmesini sağlayan süreci,

l) Sızma testi: Bilgi sistemlerindeki varsa güvenlik açıklarını, istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen atakları içeren faaliyetleri,

m) Sistem: Ödeme sistemi ve menkul kıymet mutabakat sistemini,

n) Sistem işleticisi: Sistemin günlük işleyişinden sorumlu olan ve sistem işletimi için gerekli olan faaliyet iznine sahip tüzel kişiyi,

o) Sorun: Bir veya daha fazla olayın kök nedenini,

ö) Stres testi: Bilgi sistemleri kapasitesinin, en yoğun yük durumundan daha yoğun durumlar karşısında

yeterliliğinin ölçüldüğü testi,

p) Yönetimden sorumlu kişi: Faaliyet Yönetmeliğinin 10 uncu maddesinde tanımlanan, sistem işleticisinin yönetiminden sorumlu kişileri,

r) Zafiyet taraması: Bilgi sistemleri bileşenlerindeki varsa güvenlik açıklarının önceden tespit edilmesine, tanımlanmasına ve sınıflandırılmasına yönelik olarak genellikle otomatik araçlarla gerçekleştirilen analizi,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Bilgi sistemleri yönetimine ilişkin genel hükümler

MADDE 5 – (1) Sistem işleticisi, bilgi sistemlerine ilişkin faaliyetlerini yürütürken işleyişinden sorumlu olduğu sistemin kesintisiz, güvenli, etkin ve verimli bir şekilde çalışması amacını öncelikli olarak gözetir.

(2) Sistem işleticisi, bilgi sistemlerini sistemin faaliyet konusu ile uyumlu şekilde tesis eder ve teknolojik gelişmeleri de dikkate alarak günceller.

(3) Sistem işleticisi, bilgi sistemleri yönetimine ilişkin politikaları sisteme ilişkin ana strateji ve hedefleri ile uyumlu şekilde yazılı olarak oluşturur, düzenli olarak gözden geçirir ve gerekli durumlarda günceller.

(4) Sistem işleticisi, sistemin yönetimini bilgi sistemleri yönetimini de kapsayacak şekilde, bütüncül bir yaklaşım içerisinde ve kurumsal yönetim uygulamaları çerçevesinde gerçekleştirir ve bilgi sistemleri yönetimine ilişkin unsurları organizasyon yapısı içerisinde uygun yere yerleştirir.

(5) Sistem işleticisi, bilgi sistemleri yönetimine ilişkin görev, yetki ve sorumlulukları açıkça belirler ve bilgi sistemleri yönetimi için gerekli her türlü kaynağı sağlar.

(6) Bilgi sistemleri yönetiminin bu Tebliğde yer alan hükümlere uygun şekilde yürütülmesinden sistem işleticisinin yönetim kurulu sorumludur.

Bilgi güvenliği yönetimi

MADDE 6 – (1) Sistem işleticisi, sisteme ilişkin her türlü bilgi varlığının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak amacıyla kural, ilke ve politikaları içeren bilgi güvenliği yönetim çerçevesi oluşturur.

(2) Sistem işleticisi, birinci fıkra kapsamında oluşturduğu bilgi güvenliği yönetim çerçevesine uygun bir bilgi güvenliği yönetim sistemi oluşturur.

(3) Sistem işleticisi, bilgi güvenliği yönetim sisteminin oluşturulmasına, yönetilmesine, belirli aralıklarla gözden geçirilmesine ve gerekli hallerde güncellenmesine ilişkin görev, yetki ve sorumlulukları açıkça belirler.

(4) Bilgi güvenliği yönetim sistemi kapsamında her kademedeki personelin bilgi güvenliğine ilişkin görev, yetki ve sorumlulukları açıkça belirlenir.

(5) Sistem işleticisi, sistem içerisindeki tüm bilgi varlıklarını önem seviyesini ve yasal yükümlülükleri de dikkate alarak gizlilik düzeyine göre sınıflandırır, her bir sınıftaki bilgi varlıklarına ilişkin erişim hakları ile saklama, iletme ve imha etme prosedürlerini açıkça belirler, sınıflandırma ve bununla ilgili yükümlülükler konusunda tüm personeli bilgilendirir.

(6) Bilgi güvenliği yönetim sisteminde, personelin işe başlaması, görev ve pozisyon değiştirmesi ve işten ayrılması da dahil olmak üzere personele ilişkin tüm hususlar bilgi güvenliğini etkileyen yönleriyle değerlendirilir ve gerekli tedbirler alınır.

(7) Sistem işleticisi, bilgi güvenliği yönetim sistemi kapsamında sistem ile ilgili kendi nezdindeki her türlü donanım ile altyapının ve bunlarla ilgili fiziksel çevrenin güvenliğini sağlar. Sistem işleticisi, sistem ile ilgili kendi nezdinde bulunmayan donanım ile alt yapının ve bunlarla ilgili fiziksel çevrenin güvenliğinin sağlanması için gerekli özeni gösterir.

(8) Sistem işleticisi, iç ve dış ağlar arasında sistem ile ilgili gerçekleşen her türlü iletişim sürecinin ve ana faaliyetlere ilişkin operasyonel işlemlerin, güvenlik kontrolleri ve araçları kullanılarak gerçekleşecek şekilde tasarlanmasını sağlar.

(9) Sistem işleticisi, yeni bir sistem kurması, mevcut sistem içerisinde yapısal bir değişikliğe gitmesi veya mevcut bilgi sistemlerine ilişkin geliştirme, bakım ve onarım çalışmaları yürütmesi durumunda bilgi güvenliğine gereken özeni göstermekle yükümlüdür.

(10) Bilgi güvenliği yönetim sistemine ilişkin görev, yetki ve sorumluluk verilmiş olan sistem işleticisinin yönetiminden sorumlu kişiler, bilgi güvenliği yönetim sisteminin bilgi güvenliği konusundaki mevzuata, standartlara ve birinci fıkra kapsamında oluşturulan bilgi güvenliği yönetim çerçevesine uyum durumunu sürekli olarak izler, uyumun sağlanması için gerekli tedbirleri alır ve uyum durumunu sistem işleticisinin yönetim kuruluna düzenli olarak raporlar.

(11) Sistem işleticisi, personelin bilgi güvenliği hususlarında farkındalığını arttıracak gerekli faaliyetleri yürütür.

Güvenlik açıkları ve ihlalleri

MADDE 7 – (1) Sistem işleticisi bilgi güvenliği yönetim çerçevesi ile uyumlu bir şekilde, bilgi sistemlerine yönelik olası güvenlik ihlallerinin araştırılmasını, güvenlik ihlallerinin önlenmesi için alınması gereken uygun tedbirlerin belirlenmesini, güvenlik ihlalinin gerçekleşmesi halinde ihlalin tespit edilerek zamanında müdahale edilebilmesi için gerekli tedbirlerin alınmasını, gerçekleşen güvenlik ihlallerinin ve tespit edilen güvenlik açıklarının değerlendirilerek kayıt altına alınmasını sağlar.

(2) Sistem işleticisi, sahip olduğu ve sistemle ilişkili olan tüm sunucular ile iletişim ağını ilk işletime alınmadan önce ve sonrasında düzenli aralıklarla yılda en az altı defa zafiyet taramasından geçirir. Zafiyet taramasında tespit edilen öncelikli bulguların mümkün olan en kısa süre içerisinde giderilmesi ve bu bulgular giderilinceye kadar uygun koruyucu tedbirlerin alınması sağlanır. Öncelikli olmayan bulguların makul bir süre içerisinde giderilmesi için zaman planlaması yapılır.

(3) Sistem işleticisi, gerçekleşebilecek iç ve dış tehditleri kapsayan senaryolar doğrultusunda yılda en az bir defa sızma testi gerçekleştirilmesini sağlar ve sızma testinin sonuçlarını Bankaya raporlar.

(4) Sistem işleticisi, olası ve gerçekleşmiş güvenlik ihlallerinin değerlendirilmesi ile zafiyet taraması ve sızma testleri sonucunda tespit ettiği güvenlik açıklarının giderilmesine yönelik olarak uygun tedbirleri alır ve aldığı tedbirlerin etkinlik durumunu kontrol eder.

(5) Sistem işleticisi, gerçekleşen güvenlik ihlallerini ve tespit edilen kritik güvenlik açıklarını, bunların giderilmesine yönelik alınan tedbirleri ve sonuçlarını içeren raporu yılda en az bir defa Bankaya sunar.

(6) Sistem işleticisi, gerçekleşen güvenlik ihlalleriyle ilgili delilleri en az on yıl süreyle güvenli bir şekilde muhafaza eder.

Denetim izi kayıt sistemi

MADDE 8 – (1) Sistem işleticisi, bilgi sistemlerine her türlü yetkili veya yetkisiz erişimin ve bilgi sistemlerinde sistem faaliyetleri ile ilgili gerçekleşen işlemlerin takibine imkan verecek denetim izi kayıt sistemi oluşturur.

(2) Denetim izi kayıt sisteminde tutulacak kayıtlar asgari olarak, erişimin veya işlemin niteliğine göre işlemin türü, işlemin ayırt edici tanımlayıcısı, işlem tutarı, işlem tarihi, işlem saati, kullanıcı kimlik bilgisi, erişimin veya işlemin gerçekleştiği uygulama bilgisini içerir.

(3) Denetim izleri, ayrıntılı incelemeye ve taramaya imkan verecek, denetime hazır ve güvenli bir şekilde en az on yıl süreyle saklanır.

(4) Bilgi sistemleri konusunda sistem işleticisi tarafından dış hizmet alınması halinde, dış hizmet sağlayıcısının denetim izi kayıt sisteminin bu madde hükümlerine uygunluğundan sistem işleticisi sorumludur.

Kimlik doğrulama, erişim denetimi ve inkar edilemezlik

MADDE 9 – (1) Sistem işleticisi, bilgi sistemlerinde gerçekleştirilen işlemlerde kullanılmak üzere yeterli ve etkin bir kimlik doğrulama sistemi kurar.

(2) Sistem işleticisi, kimlik doğrulama sisteminin bilgi sistemlerinin hangi alt bileşenleri için geçerli olacağını ve kimlik doğrulama sisteminde hangi alt bileşen için hangi kimlik doğrulama tekniklerinin kullanılacağını açıkça belirler.

(3) Sistem işleticisi, personelin sistem içerisinde kullanılan ağlara, alt sistemlere, uygulamalara, verilere ve fiziksel ortamlara erişimine ilişkin yetki ve sınırlandırmaları, personelin görev, yetki ve sorumlulukları kapsamında işin gerektirdiği bilgiye erişimine imkan verecek şekilde açıkça belirler ve yetkisiz erişimleri engellemek üzere gerekli tedbirleri alır.

(4) Sistem işleticisi, kimlik doğrulama için kullanılan verilerin güvenliği ile şifreli olarak aktarılması ve tutulması için gerekli altyapının oluşturulmasını sağlar.

(5) Sistem işleticisi, bilgi sistemlerinin kullanımında oturum güvenliğini sağlayacak tedbirleri alır.

(6) Sistem işleticisi, bilgi sistemlerinde sistem faaliyetleri ile ilgili gerçekleştirilen işlemler için inkar edilemezliği sağlayacak teknolojik ve hukuki altyapıyı oluşturur.

Bilgi sistemlerine ilişkin risk yönetimi

MADDE 10 – (1) Sistem işleticisi, sistemin sorunsuz şekilde işlemesini tehlikeye sokabilecek tüm risklerin tespit edilmesini, ölçülmesini, izlenmesini ve etkin bir şekilde yönetilmesini sağlamak amacıyla tesis edeceği risk yönetim çerçevesini oluştururken, bilgi sistemlerine ilişkin riskleri göz önünde bulundurur.

(2) Birinci fıkra uyarınca bilgi sistemlerine ilişkin riskler değerlendirilirken, sistemin ana faaliyetleri ile diğer faaliyetleri, sisteme doğrudan veya dolaylı olarak bağlanan katılımcıların veya diğer kuruluşların faaliyetleri, varsa dış hizmet sağlayıcıların faaliyetleri, üçüncü taraflara olan bağımlılıklar ve sistemin diğer sistemlerle olan bağlantıları da göz önünde bulundurulur.

(3) Sistem işleticisi, yılda en az bir defa bilgi sistemlerine ilişkin kapsamlı bir risk değerlendirmesi yapar ve değerlendirme sonuçlarını içerir raporu Bankaya sunar.

Bilgi sistemleri işletimi

MADDE 11 – (1) Sistem işleticisi, tanımlanan hizmet seviyeleri çerçevesinde bilgi sistemlerinin işleyişinin güvenilirliğine, dayanıklılığına ve sürekliliğine ilişkin hedefleri açıkça belirler ve bu hedefler doğrultusunda bilgi sistemlerinin işletiminin etkin ve verimli yapılabilmesi amacıyla gerekli tedbirleri alır.

(2) Sistem işleticisi birinci fıkra kapsamında belirlediği hedeflere uyum düzeyini yılda en az bir defa olmak üzere düzenli aralıklarla ölçer ve sonuçlarını Bankaya raporlar.

(3) Sistem işleticisi, bilgi sistemlerini tanımlanan hizmet seviyeleri için yeterli kapasiteye sahip olacak şekilde tesis eder, kapasitenin ölçeklenebilir olmasını öncelikli olarak gözetir ve bilgi sistemlerine yönelik kapasite yönetimi yapar.

(4) Sistem işleticisi, bilgi varlıklarının envanterinin ve konfigürasyon bilgisinin oluşturulmasını, güvenli bir şekilde saklanmasını, güncellenmesini ve raporlanmasını sağlar.

(5) Sistem işleticisi, önceden belirlenmiş prosedürler çerçevesinde olayların zamanında tespit edilmesini, kayıt altına alınmasını, raporlanmasını, analiz edilmesini, çözülmesini ve olay hakkında ilgili tüm paydaşların zamanında bilgilendirilmesini sağlayacak şekilde olay yönetimi yapar.

(6) Sistem işleticisi, her önemli olaydan sonra olayın ayrıntılı olarak incelenmesini, kök neden analizinin yapılmasını, etkilerinin belirlenmesini ve olaya ilişkin sorunun takibini ve raporlamasını içerecek şekilde sorun yönetimi yapar.

(7) Sistem işleticisi, bilgi sistemleri ile ilgili yapılacak her türlü değişikliği, belirlemiş olduğu değişiklik yönetimi prosedürlerine uygun olarak gerçekleştirir.

(8) Sistem işleticisi, kurum içi geliştirme veya dış alım yoluyla bilgi sistemlerinde gerçekleştirilecek her türlü projeyi, belirlemiş olduğu proje yönetimi prosedürlerine uygun olarak yürütür.

Bilgi sistemleri süreklilik planı

MADDE 12 – (1) Sistem işleticisi, Faaliyet Yönetmeliğinin 25 inci maddesinin beşinci fıkrası uyarınca oluşturulan iş sürekliliği planının bir parçası olarak bilgi sistemleri süreklilik planı hazırlar.

(2) Bilgi sistemleri süreklilik planı;

a) İş sürekliliği planı ile uyumlu olacak şekilde belirlenecek bilgi sistemleri süreklilik hedeflerini ve bu hedeflere ulaşmayı sağlamak üzere oluşturulacak yedekleme ve hatadan kurtarma prosedürleri ile kullanılacak kaynakları,

b) Planın hayata geçmesine neden olan olayın kaynağını, yarattığı hasarı, potansiyel boyutunu ve etkisini, etkilediği tarafları tespit etmeye ve tespitlerin ilgili yönetim birimlerine ulaştırılmasını sağlamaya yönelik süreçleri,

c) Planın hayata geçirilmesine ilişkin karar alma süreciyle ilgili kriter ve prosedürler ile plan devreye girdiğinde rol alacak kişi veya grupların görev, yetki ve sorumluluklarını,

ç) İlgili paydaşlar ile iletişim yöntemini,

d) Plan kapsamında verilen kararların ve hayata geçirilen eylemlerin kayıt altına alınma yöntemini

içerir.

(3) Sistem işleticisi, bilgi sistemleri süreklilik planının etkinliğini yılda en az bir defa test eder. Sistem işleticisi, bu testleri katılımcıları, bilgi sistemlerine bağlantısı bulunan diğer sistemleri ve üçüncü taraf hizmet sağlayıcıları da dahil edecek şekilde planlar.

Bilgi sistemlerine ilişkin dış hizmet alımı

MADDE 13 – (1) Sistem işleticisi, bilgi sistemlerine ilişkin dış hizmet alımı gerçekleştirebilir. Dış hizmet alınması sistem işleticisinin bilgi sistemleri yönetimi kapsamındaki sorumluluklarını ortadan kaldırmaz.

(2) Sistem işleticisi, dış hizmet alımı nedeniyle ortaya çıkabilecek riskleri değerlendirir ve gerekli tedbirleri alır.

(3) Dış hizmet alım sözleşmesi asgari olarak;

a) Hizmetin kapsamına ve belirlenen hizmet seviyelerine ilişkin hususları,

b) Hizmetin sona ermesine ilişkin şartları ve hizmetin sona ermesi durumunda dış hizmet sağlayıcısının dış hizmet sunarken elde ettiği bilgi, belge ve kayıtları imha etmesine ilişkin hükümleri,

c) Sistem işleticisi ile dış hizmet sağlayıcısının hak ve yükümlülüklerini,

ç) Dış hizmet sağlayıcısının hizmete ilişkin kullandığı kaynakların ve süreçlerin sistem işleticisinin güvenlik politikalarına uygun olmasını sağlayacak hükümleri,

d) Sözleşmeye konu unsurların sahipliğine ve fikri mülkiyet haklarına ilişkin hususları,

e) Dış hizmet alımı yoluyla gerçekleştirilen işlemlere ilişkin bilgi, belge ve kayıtların mülkiyetinin sistem işleticisine ait olduğuna ve sistem işleticisine ait bilgi, belge ve kayıtların gizliliğine ilişkin hükümleri,

f) Sözleşme hükümlerinin, dış hizmet sağlayıcısının varsa alt yüklenicileri ile olan sözleşmelerinde de bağlayıcı olmasına dair hükümleri,

g) Sistem işleticisinin, sistem işleticisi olma vasfı nedeniyle tabi olduğu mevzuat ve Banka talimatları uyarınca bilgi sistemlerinde gerçekleştirilmesi gereken değişikliklerin alınan hizmet kapsamında dış hizmet sağlayıcısı tarafından yerine getirilmesini sağlayacak hükümleri,

ğ) Dış hizmet sağlayıcısı yoluyla gerçekleştirilen faaliyetlerin de Banka tarafından sistem işleticisine yönelik yürütülecek gözetim faaliyeti kapsamında yer aldığına ve dış hizmet sağlayıcısından talep edilen her türlü bilgi, belge ve kaydı zamanında ve doğru olarak vermek ve bunlara erişim için gerekli olan her türlü imkanı sağlamak zorunda olduğuna dair hükümleri,

h) Sözleşme hükümlerinin herhangi bir nedenle ihlali durumunda izlenecek prosedürlere ilişkin hükümleri,

içerir.

(4) Sistem işleticisinin verilerin işlenmesi ve saklanması için dış hizmet alması durumunda, bu hizmet sadece sistem işleticisine tahsis edilmiş donanımlar üzerinden sunulur.

(5) Sistem işleticisi, dış hizmet alımlarında kendi bilgileri ve katılımcılarının bilgilerinin güvenliğini sağlayacak gerekli tedbirleri alır ve dış hizmet sağlayıcısına sadece işin gerektirdiği bilgiye erişim imkanı sağlayacak şekilde erişim yetkisi verir.

ÜÇÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Uygulama esasları

MADDE 14 – (1) Banka, bu Tebliğ hükümlerini yorumlamaya, bu Tebliğde yer almayan ya da açıklık bulunmayan konularda genel hükümleri de göz önünde bulundurarak karar vermeye, uygulamayı düzenlemek ve yönlendirmek için genelge ve talimat yayımlamaya yetkilidir.

Geçiş hükmü

GEÇİCİ MADDE 1 – (1) Sistem işleticileri, sistemlerini bu Tebliğin yayımından itibaren bir yıl içinde bu Tebliğ ile uyumlu hâle getirmek zorundadır.

Yürürlük

MADDE 15 – (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16 – (1) Bu Tebliğ hükümlerini Türkiye Cumhuriyet Merkez Bankası Başkanı yürütür.