Ödeme ve Elektronik Para Kuruluşlarına Topluluk Bulutu Hizmeti Sunan Dış Hizmet Sağlayıcılara İlişkin Rehber

Ödeme Sistemleri ve Finansal Teknolojiler Genel Müdürlüğü

Temmuz 2022

TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sürüm Tarihçesi

Güncelleme Tarihi	Güncelleme Açıklaması	Sürüm
Temmuz 2022	İlk Sürüm	1.0

1 Aralık 2021 tarih ve 31676 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ'in (Tebliğ) 16'ncı maddesinin yedinci fıkrasında,

" *(7) Kuruluş her türlü veriyi işlemek, saklamak ve iletmek için bir dış hizmet olarak yurt içinde tesis edilmiş bulut bilişim hizmetlerini kullanabilir. Ancak hassas müşteri verilerini, rekabete duyarlı verileri, kişisel verileri veya müşteriyle ilintilendirilebilir ve onu belirli ya da belirlenebilir kılan her türlü bilgiyi işleyecek, saklayacak ve iletecek şekilde bulut bilişim hizmetinin alınması, bu dış hizmetin ancak sadece kuruluşa tahsis edilmiş donanım ve yazılım kaynakları üzerinden sunulduğu özel bulut hizmet modeli ile alınması halinde mümkündür.* ***Banka tarafından uygun görülen dış hizmet sağlayıcılar tarafından sunulması durumunda*** *kuruluş, sadece ödeme hizmeti sağlayıcılarına veya bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen diğer kredi kuruluşları veya finansal kuruluşlara tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın atandığı topluluk bulutu hizmet modeliyle dış hizmet alabilir. Topluluk bulutu hizmetinin, kuruluşun ana ortağı, iştiraki veya ana ortağının iştiraki olan ve bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen bir kredi kuruluşu veya finansal kuruluş tarafından verilmesi, sadece ana ortak, iştirakleri ve ana ortağın iştiraklerine tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal ayrıma gidilerek kuruluşa özgü ayrı bir kaynak atanması koşuluyla bu fıkra hükümlerine aykırılık teşkil etmez. Kuruluşun müşteri verisi içermeyen test ve geliştirme ortamları ve sistemleri için gerekli güvenlik tedbirlerini alarak bulut bilişim hizmeti alması halinde bu fıkra hükmü uygulanmaz*",

hükmü yer almaktadır. Anılan hüküm uyarınca, donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın mantıksal olarak atandığı topluluk bulutu hizmet modeliyle dış hizmet alımı, sadece anılan donanım ve yazılım kaynağının ödeme hizmeti sağlayıcılarına veya bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen diğer kredi kuruluşları veya finansal kuruluşlara tahsis edilmiş olması ve söz konusu hizmeti sunan dış hizmet sağlayıcısına Türkiye Cumhuriyet Merkez Bankası (Banka) tarafından uygunluk verilmesi şartları ile mümkün bulunmaktadır.

Bu rehberde, yukarıda belirtilen şekilde topluluk bulutu hizmeti verecek dış hizmet sağlayıcıların uygunluk alabilmesi için yerine getirmesi gereken şartlar ile başvuru, değerlendirme ve gözetim süreçlerine ilişkin önemli hususlar yer almakta olup Banka tarafından değerlendirmeler çerçevesinde ihtiyaç duyulması durumunda rehberde yer alan hususların uygulanması aşamasında değişiklik yapılması veya ilave bilgi ve belge talep edilmesi mümkün bulunmaktadır.

A. UYGUNLUK ŞARTLARI

Tebliğ'in 16'ncı maddesinin yedinci fıkrası uyarınca, ödeme ve elektronik para kuruluşlarına (Kuruluş) donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın atandığı topluluk bulutu hizmet modeliyle hizmet sunmak isteyen dış hizmet sağlayıcı;

1. a. Yetkili bir otorite tarafından düzenlenen bir kredi kuruluşu veya finansal kuruluş ya da bunların ana ortağı olduğu özel hukuk tüzel kişisi olması,

   b. Kanun ile kurulmuş bir birlik nezdinde faaliyet göstermesi,

   c. 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun'un 3'üncü maddesinin birinci fıkrasında tanımlanan bir elektronik haberleşme işletmecisi veya bunların ana ortağı olduğu bir kuruluş ya da özel hukuk tüzel kişisi olması,

   d. Özel kanunla veya Cumhurbaşkanlığı kararnamesiyle kurulmuş sanayi-teknoloji alanlarında faaliyet gösteren bir kamu kurumu, kuruluşu, vakıf veya bunların ana ortak olduğu sanayi-teknoloji alanında faaliyet gösteren özel hukuk tüzel kişisi olması

   şartlarından en az birini sağlaması,

2. Topluluk bulut hizmetinin bizzat kendisiyle ilgili faaliyetleri dış hizmet alımına konu etmemesi,

3. Sunulan hizmetlerin kesintisiz, güvenli, etkin ve verimli bir şekilde sürdürülmesini sağlamak amacıyla;

   a. Operasyon/izleme ekibi, altyapı ekibi ve bilgi güvenliği ekibinin her biri için, en az 1'er (birer) kişisi benzer alanlarda asgari 7 (yedi) yıl tecrübeye sahip olmak üzere, yeterli sayıda ve yetkinlikte personel istihdam edilmesi,

   b. Gerekli bilgi sistemlerini ve teknolojik altyapıyı kurması,

4. Aşağıda belirtilen ve geçerliliği devam eden sertifikalara sahip olması:

   a. Birincil merkeze ait Tier 3 veya Tier 4 veri merkezi altyapı sertifikası bulunması, ikincil merkeze ait Tier 3 veya Tier 4 veri merkezi altyapı sertifikası yoksa bu sertifikaları karşılayacak gereksinimleri sağlamış olması,

   b. ISO/IEC 27001 veya TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası,

   c. ISO 22301 veya TS EN ISO 22301 İş Sürekliliği Yönetimi sertifikası,

5. Bilgi sistemlerinin, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından, gerçekleşebilecek iç ve dış tehditleri kapsayan senaryolar doğrultusunda ve Tebliğ eklerinden "Ek-5: Bilgi Sistemleri Sızma Testleri Usul ve Esasları"na uygun olarak başvurunun yapıldığı tarih itibarıyla geçmiş bir yıl içerisinde sızma testi gerçekleştirilmiş olması, tespit edilen öncelikli bulguların giderilmiş olması,

6. Bilgi sistemlerinin sorunsuz şekilde işlemesini tehlikeye sokabilecek, üçüncü taraflara bağımlılıklar da dâhil olmak üzere, tüm risklerin tespit edilmesini, ölçülmesini, izlenmesini ve etkin bir şekilde yönetilmesini sağlamak amacıyla uygulanması gereken önlemlere ilişkin usul ve esaslar ile tesis

edilmesi gereken kontrolleri içerir politika, prosedür ve süreç dokümanlarının yazılı olarak oluşturulması ve üst yönetim tarafından onaylanmış bir risk yönetim çerçevesinin bulunması,

7. Topluluk bulutu hizmetine özgülenen birincil ve ikincil sistemleri ile veri yedekleme merkezlerinin yurt içinde bulunması,
8. Bankaca ihtiyaç görülmesi halinde Banka teknik ekibi tarafından yapılacak yerinde inceleme sonucunda, kuruluşun ve dış hizmet sağlayıcının Tebliğe uyumluluğu kapsamında herhangi bir olumsuzluk ve eksiklik tespit edilmemiş olması

şartlarını yerine getirir.

B. UYGUNLUK BAŞVURUSU

1. Tebliğ'in 16'ncı maddesinin yedinci fıkrası uyarınca, kuruluşlara donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın mantıksal olarak atandığı topluluk bulutu hizmet modeliyle hizmet sunmak isteyen dış hizmet sağlayıcı aşağıda belirtilen bilgi ve belgeler ile Bankaya yazılı olarak başvuru yapar:
    a. Bu rehberin Uygunluk Şartları bölümünde yer alan gereksinimleri yerine getirdiğini gösterir belgeler,
    b. Uygunluk Şartları bölümünde yer alan 6'ncı madde kapsamında son bir yıl içerisinde gerçekleştirilmiş risk değerlendirme raporu,
    c. Bilgi sistemleri mimarisi ile ağ topolojisini gösterir belgeler,
    d. Yönetim ve organizasyon şeması ile personel bilgisi,
    e. Alınan dış hizmetlere ilişkin bilgiler,
    f. Dış hizmet sağlayıcı olarak sunduğu hizmetlere ilişkin bilgiler,
    g. Halihazırda (varsa) dış hizmet verilen kuruluşlar ve bu kuruluşlara verilen hizmetlere ilişkin bilgiler,
    h. Topluluk bulutu kapsamında sunulan ve/veya sunulması planlanan hizmetler ve (varsa) hizmet paketleri,
    i. İletişim bilgileri.
2. Banka, yukarıda belirtilen bilgi ve belgelerde eksiklik bulunması durumunda başvuruyu değerlendirmeye almaz ve bununla ilgili olarak dış hizmet sağlayıcıyı yazılı olarak bilgilendirerek eksikliğin giderilmesi için 30 (otuz) günü geçmeyecek şekilde makul süre verir.
3. Eksik bilgi ve belgelerin verilen süre içerisinde dış hizmet sağlayıcı tarafından Bankaya iletilmemesi durumunda başvuru süreci olumsuz olarak değerlendirilir.

C. UYGUNLUK DEĞERLENDİRME

Dış hizmet sağlayıcının, başvuru için gerekli bilgi ve belgeleri eksiksiz olarak iletmesinin ardından Banka tarafından uygunluk değerlendirme süreci başlatılır.

1. Uygunluk değerlendirme süreci boyunca ihtiyaç duyulması durumda Uygunluk Şartları bölümünde yer alan 8'inci koşul kapsamında Bankaca yerinde inceleme (birincil merkez ve/veya ikincil merkezleri de kapsayabilecek şekilde) yapılması mümkün bulunmaktadır. Dış hizmet sağlayıcı, yerinde inceleme süresince banka ekibi tarafından talep edilen bilgi ve belgeleri sağlamakla yükümlüdür.
2. Banka, değerlendirme süreci boyunca dış hizmet sağlayıcıdan ek bilgi ve belge isteyebilir.
3. Banka, değerlendirmesini tamamlamasını müteakip başvuru sahibi dış hizmet sağlayıcıya sonucu yazılı olarak bildirir.

D. UYGUNLUK GÖZETİMİ

Tebliğ'in 16'ncı maddesinin yedinci fıkrası uyarınca, ödeme ve elektronik para kuruluşlarına donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın mantıksal olarak atandığı topluluk bulutu hizmet modeliyle hizmet sunabilmesi için, uygunluk verilen dış hizmet sağlayıcı uygunluk verilmesinin ardından aşağıda belirtilen hususları yerine getirmekle yükümlüdür.

1. Dış hizmet sağlayıcı, Uygunluk Başvurusu bölümünün 1'nci maddesinde yer alan bilgi ve belgelerde meydana gelen önemli değişiklikleri gecikmeksizin Bankaya yazılı olarak bildirir. Her halûkarda, söz konusu belgelerin güncel hallerini uygunluk verilen tarihten itibaren asgari iki yılda bir kez olmak üzere Bankaya iletir.
2. Dış hizmet sağlayıcı, ihtiyaç halinde Banka tarafından talep edilen ilave bilgi ve belgeleri Bankaca belirlenen makul süre içerisinde Bankaya sunmakla yükümlüdür.
3. Banka, gerek görmesi halinde yerinde inceleme yapabilir ve/veya kapsamı Bankaca belirlenecek şekilde bağımsız denetim yaptırılmasını isteyebilir. Söz konusu denetim faaliyeti Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayımlanan Bankalarda Bilgi Sistemi Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bağımsız denetim kuruluşlarınca yapılır.
4. Dış hizmet sağlayıcı, uygunluk onayının alındığı yıldan sonraki her takvim yılı içerisinde en az bir kez olmak üzere bu rehberin Uygunluk Şartları bölümünün 5'inci maddesinde belirtilen sızma testini gerçekleştirir. Dış hizmet sağlayıcı, gerçekleşen güvenlik ihlallerini, sızma testinin sonuçlarını ve tespit edilen kritik güvenlik açıklarını, bunların giderilmesine yönelik alınan tedbirleri ve sonuçlarını içeren raporu yılda en az bir defa olmak üzere hazırlar, üst yönetimine onaylatır ve Bankanın talep etmesi durumunda Bankaya iletir.
5. Dış hizmet sağlayıcı, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce ve yılda en az bir defa olmak üzere bilgi sistemlerine ilişkin kapsamlı bir risk değerlendirmesi yapar. Risk

değerlendirme sonuçlarını ve bunlara ilişkin alınacak aksiyonları içerir raporu her yıl Ocak ayı sonuna kadar bir önceki yıla ilişkin olacak şekilde hazırlar, üst yönetimine onaylatır ve Bankanın talep etmesi durumunda Bankaya iletir.

6. Dış hizmet sağlayıcı, donanım ve yazılım kaynaklarının fiziksel olarak paylaşımını sağladığı kaynağa yeni bir kurum/kuruluşu dâhil etmeden önce bu durumu ve verilecek hizmetin mahiyetini detaylı olarak Bankaya bildirmek ve Bankanın onayını almakla yükümlüdür.

7. Banka, bu rehberde yer alan gereksinimlere uygunluk koşullarının bozulması durumunda, dış hizmet sağlayıcıya Tebliğ'in 16'ncı maddesinin yedinci fıkrası kapsamında verilen uygunluğu iptal edebileceği gibi; söz konusu dış hizmet sağlayıcıyı gerekli uyumu sağlaması için yazılı olarak uyarabilir ve uyarının iletildiği tarihten itibaren 6 (altı) ayı geçmeyecek şekilde verilen makul süre içerisinde eksikliklerin giderilmesini isteyebilir.

8. Dış hizmet sağlayıcı, topluluk bulutu hizmeti kapsamında olağan işleyişi aksatan, kesintiye sebep olan veya verilerin işlenmesini, saklanmasını ve iletilmesini engelleyen yapısal sorun veya kesintileri gecikmeksizin Bankaya bildirir.