

Ödeme ve İşlem Güvenliği Politikası

OTOVİM TEKNOLOJİ A.Ş. · Yürürlük tarihi: 26.10.2026 · Sürüm 2 · Kanıt: 62530cb6f7676873...

YEDEKNOKTA.COM

ÖDEME, İŞLEM GÜVENLİĞİ VE İADE/CHARGEBACK POLİTİKASI

MADDE 1 - AMAÇ

İşbu Ödeme, İşlem Güvenliği ve İade/Chargeback Politikası'nın ("Politika") amacı; OTOVİM Teknoloji Anonim Şirketi ("Yedeknokta") tarafından işletilen Yedeknokta.com Platformu üzerinden gerçekleştirilen ödeme işlemlerinin;

- güvenli,
- izlenebilir,
- mevzuata uygun,
- dolandırıcılık risklerini azaltacak,
- kullanıcı ve Satıcı haklarını koruyacak

şekilde yürütülmesine ilişkin temel esasları belirlemektir.

Politika ayrıca;

- ödeme hizmetleri,
- sanal POS kullanımı,
- ödeme hizmeti sağlayıcıları,
- kart güvenliği,
- PCI DSS,
- işlem izleme,
- dolandırıcılık önleme,
- para iadeleri,
- chargeback/ters ibraz,
- Satıcı hakedişleri,
- şüpheli ödeme işlemleri,
- ödeme güvenliği olayları

bakımından uygulanacak temel süreçleri düzenler.

MADDE 2 - KAPSAM

İşbu Politika;

- Alıcı ödemelerini,
- kredi/banka kartı işlemlerini,
- sanal POS işlemlerini,
- ödeme hizmeti sağlayıcısı entegrasyonlarını,
- para iadelerini,
- iptal işlemlerini,
- chargeback süreçlerini,
- Satıcı hakediş ve ödeme süreçlerini,
- işlem güvenliği kontrollerini,
- ödeme dolandırıcılığı incelemelerini

kapsar.

MADDE 3 - POLİTİKANIN NİTELİĞİ

İşbu Politika, Yedeknokta'nın ödeme ve işlem güvenliği süreçlerine ilişkin esasları belirler; tüketicilerin emredici mevzuattan doğan haklarını veya Yedeknokta'nın kanundan doğan yükümlülüklerini ortadan kaldırmaz.

Tüketicilerin ödeme, iptal ve para iadesine ilişkin hakları ayrıca;

- Ön Bilgilendirme Formu,
- Mesafeli Satış Sözleşmesi,
- Teslimat, Cayma, İade ve Satış Sonrası Politikası

kapsamında düzenlenir.

MADDE 4 - TEMEL İLKELER

Ödeme süreçlerinde aşağıdaki ilkeler esas alınır:

1. Güvenli ödeme altyapısı kullanılması,
2. Gereksiz kart verisinin toplanmaması,
3. Yetkisiz erişimin önlenmesi,
4. İşlemlerin kayıt altına alınması,
5. Dolandırıcılık riskinin izlenmesi,
6. Para iadelerinin izlenebilir olması,
7. Chargeback süreçlerinin belgeli yürütülmesi,
8. Görevler ayrılığı,
9. Kullanıcının yanıtılmaması,

10. Satıcı ve ödeme kuruluđu kayıtlarının mutabakatının sağlanması.

MADDE 5 - YEDEKNOKTA’NIN ÖDEME SÜRECİNDEKİ KONUMU

Yedeknokta’nın ödeme işlemlerindeki hukuki ve teknik rolü kullanılan iş modeline göre belirlenir.

Yedeknokta;

- yetkili banka,
- ödeme hizmeti sağlayıcısı,
- elektronik para kuruluđu,
- sanal POS sağlayıcısı

tarafından sunulan altyapıları kullanabilir.

Yedeknokta’nın yalnızca elektronik ticaret platformu olarak faaliyet gösterdiği ve ödeme hizmetinin yetkili banka, ödeme kuruluđu veya elektronik para kuruluđu tarafından sunulduğu hallerde, Yedeknokta kendisini ödeme hizmeti sağlayıcısı olarak tanıtmaz; fonların tahsili, korunması, aktarılması ve ödeme işleminin gerçekleştirilmesine ilişkin yükümlölükler ilgili yetkili kuruluđun sorumluluk alanındadır.

MADDE 6 - YETKİLİ ÖDEME HİZMETİ SAĞLAYICILARI

Ödeme işlemlerinde kullanılacak üçüncü taraf sağlayıcıların;

- gerekli faaliyet yetkilerine sahip olması,
- güvenlik seviyesinin yeterli olması,
- sözleşmesel yükümlölüklerinin açık olması,
- olay bildirim mekanizmasının bulunması

kontrol edilir.

MADDE 7 - ÖDEME SAĞLAYICISI ENVANTERİ

Aşağıdaki bilgiler şirket içinde güncel tutulur:

Sağlayıcı	Hizmet	Sözleşme Tarihi	Teknik Entegrasyon	Veri İşleme	Yurt Dışı Aktarım	Sorumlu
[●]	Sanal POS	[●]	[●]	[●]	[●]	[●]

Sağlayıcı	Hizmet	Sözleşme Tarihi	Teknik Entegrasyon	Veri İşleme	Yurt Dışı Aktarım	Sorumlu
[●]	Ödeme Aracısı	[●]	[●]	[●]	[●]	[●]

MADDE 8 - ÖDEME SAĞLAYICISI SÖZLEŞME KONTROLÜ

Ödeme hizmeti sağlayıcılarıyla yapılan sözleşmelerde mümkün olduğu ölçüde;

- hizmet kapsamı,
- işlem ücretleri,
- ödeme aktarım süreleri,
- chargeback süreçleri,
- fraud işlemleri,
- veri güvenliği,
- veri ihlali bildirimi,
- hizmet kesintisi,
- sorumluluk,
- sözleşmenin sona ermesi,
- veri iadesi/silme

hususları düzenlenir.

MADDE 9 - KABUL EDİLEN ÖDEME YÖNTEMLERİ

Platform'da aşağıdaki ödeme yöntemlerinden uygun olanları sunulabilir:

- kredi kartı,
- banka kartı,
- banka transferi,
- ödeme kuruluşu aracılığıyla ödeme,
- mevzuata uygun diğer elektronik ödeme yöntemleri.

Aktif ödeme yöntemleri kullanıcıya ödeme ekranında açıkça gösterilir.

MADDE 10 - ÖDEME EKRANI

Ödeme işlemi tamamlanmadan önce Alıcıya en az;

- ürün bedeli,

- kargo bedeli,
- indirim,
- varsa diğ er  cretler,
- toplam  denecek tutar,
-  deme y ntemi

g sterilir.

Alıcının  deme y k ml l ğ  doğuran i lemi a ık  ekilde anlaması saėlanır;  deme onayı, i lem  zeti ve  deme ba arısı veya ba arısızlıėına ili kin kayıtlar ispat ve uy  mazlık y netimi amacıyla hukuka uygun  ekilde muhafaza edilir.

MADDE 11 - KART VERİSİ G VENLİĐİ

Yedeknokta'nın  deme mimarisi m mk n olduėu  l  de tam kart verisinin Yedeknokta sistemlerine girmeyeceėi  ekilde yapılandırılır.

Kart bilgilerinin doėrudan yetkili  deme hizmeti saėlayıcısının g venli  deme ekranı veya altyapısı  zerinden i lenmesi tercih edilir.

MADDE 12 - KART BİLGİLERİNİN SAKLANMASI

Yedeknokta'nın operasyonel ihtiya ı bulunmadık a;

- tam kart numarası,
- kart g venlik kodu/CVV/CVC,
- manyetik  erit verileri,
- PIN bilgisi

saklanmaz.

 deme saėlayıcısının kart saklama/tokenizasyon hizmeti kullanılıyorsa Yedeknokta m mk n olduėu  l  de ger ek kart verisi yerine token kullanır.

MADDE 13 - CVV/CVC VERİSİ

Kart g venlik kodlarının i lem sonrasında saklanmaması esastır.

 deme sistemi bu verinin Yedeknokta loglarına veya uygulama kayıtlarına yazılmasına izin vermeyecek  ekilde yapılandırılır.

MADDE 14 - TOKENİZASYON

Kayıtlı kart veya tekrarlayan  deme  zelliėi sunulması halinde, m mk n olduėu  l  de kart bilgileri yetkili  deme saėlayıcı nezdinde tutulur ve Yedeknokta sistemlerinde yalnızca token

veya benzeri güvenli tanımlayıcı saklanır.

MADDE 15 - PCI DSS

Kart verilerinin işlendiği ödeme altyapılarında PCI DSS kapsamı kullanılan teknik mimariye göre değerlendirilir.

Yedeknokta;

- kart verisini doğrudan işlemiyorsa dahi kendi sorumluluk alanını,
- ödeme sağlayıcısının PCI DSS durumunu,
- entegrasyon güvenliğini,
- ödeme sayfasında kullanılan teknik bileşenleri

gerektiğinde kontrol eder.

İşbu Politika, Yedeknokta'nın kendiliğinden PCI DSS sertifikasına sahip olduğu anlamına gelmez.

MADDE 16 - PCI DSS KAPSAM KONTROLÜ

Periyodik olarak aşağıdaki sorular değerlendirilir:

- Kart verisi Yedeknokta sunucularından geçiyor mu?
- Kart verisi Yedeknokta sistemlerinde saklanıyor mu?
- Ödeme ekranı üçüncü taraf sağlayıcı tarafından mı sunuluyor?
- Tokenizasyon kullanılıyor mu?
- Kart verisi loglara yazılıyor mu?
- Ödeme sağlayıcısının PCI DSS durumu kontrol edildi mi?
- Teknik entegrasyonda sonradan değişiklik yapıldı mı?

MADDE 17 - GÜVENLİ İLETİŞİM

Ödeme işlemlerinde kullanıcı ile sistem arasında veri aktarımı güvenli iletişim protokolleri üzerinden gerçekleştirilir.

Güncel olmayan veya güvenli kabul edilmeyen şifreleme yöntemlerinin kullanımından kaçınılır.

MADDE 18 - ÖDEME SİSTEMİNE ERİŞİM

Ödeme yönetim paneli, sanal POS ve benzeri kritik sistemlere erişim yalnızca görev gereği yetkili personele sağlanır.

Mümkün olduğu ölçüde;

- MFA,
- rol bazlı erişim,
- ayrı kullanıcı hesabı,
- erişim logu

kullanılır.

MADDE 19 - PAYLAŞIMLI ÖDEME HESAPLARI

Ödeme yönetim sistemlerinde ortak kullanıcı adı/parola kullanımından kaçınılır.

Her kullanıcının işleminin kişisel kullanıcı hesabıyla izlenebilir olması tercih edilir.

MADDE 20 - GÖREVLER AYRILIĞI

Mümkün olduğu ölçüde;

- para iadesi talebini oluşturan,
- yüksek tutarlı iadeyi onaylayan,
- Satıcı banka hesabı değiştiren,
- Satıcı hakedişini serbest bırakan

kişilerin aynı kişi olmaması sağlanır.

MADDE 21 - YÜKSEK TUTARLI İŞLEMLER

Şirket tarafından belirlenecek [●] TL üzerindeki;

- manuel para iadeleri,
- Satıcı ödemeleri,
- ödeme düzeltmeleri

için ikinci onay mekanizması uygulanabilir.

MADDE 22 - 3D SECURE VE EK DOĞRULAMA

Ödeme sağlayıcısının desteklediği ve risk değerlendirmesinin gerekli gördüğü durumlarda 3D Secure veya benzeri ek doğrulama mekanizmaları kullanılabilir.

Ek doğrulamanın hangi işlemlerde zorunlu tutulacağı;

- işlem tutarı,
- fraud riski,
- ödeme sağlayıcısı kuralları,
- kullanıcı deneyimi,

- kart kuruluđu/banka gereklilikleri

dikkate alınarak belirlenir.

MADDE 23 - İŞLEM İZLEME

Ödeme işlemleri dolandırıcılık ve kötüye kullanım riskleri bakımından izlenebilir.

İzleme kapsamında örneğin;

- kısa sürede çok sayıda ödeme denemesi,
- çok sayıda başarısız kart denemesi,
- olağandışı yüksek tutar,
- aynı hesapta çok sayıda farklı kart,
- aynı kartla çok sayıda farklı hesap,
- teslimat ve fatura bilgilerinde olağandışı uyumsuzluk,
- yüksek riskli cihaz veya IP davranışı,
- çok sayıda iptal/iade/chargeback

gibi göstergeler değerlendirilebilir.

MADDE 24 - RİSK SKORLAMA

İşlemler şirketin teknik imkanları dahilinde risk seviyesine göre sınıflandırılabilir.

Düşük Risk

Olağan kullanıcı ve işlem davranışı.

Orta Risk

Ek kontrol gerektiren ancak açık dolandırıcılık göstergesi bulunmayan işlem.

Yüksek Risk

Birden fazla güçlü dolandırıcılık göstergesi bulunan işlem.

Risk skoru tek başına kesin suç veya dolandırıcılık tespiti olarak kabul edilmez.

MADDE 25 - YÜKSEK RİSKLİ İŞLEMLER

Yüksek riskli işlem tespit edildiğinde;

- ek kimlik doğrulama,
- siparişin geçici incelemeye alınması,
- ödeme sağlayıcısından ek kontrol,
- manuel inceleme,

- siparişin hukuka uygun şekilde iptali

uygulanabilir.

Tedbirler işlem riskiyle ölçülü olmalıdır.

MADDE 26 - OTOMATİK RED KARARLARI

Fraud önleme sistemleri kullanılması halinde otomatik kuralların gerçek kullanıcıların sistematik olarak haksız biçimde engellenmesine yol açmaması için periyodik kontrol yapılır.

Gerekli olduğu ölçüde manuel inceleme mekanizması oluşturulur.

MADDE 27 - FRAUD GÖSTERGELERİ

Aşağıdaki durumlar ek inceleme sebebi olabilir:

- çok sayıda başarısız ödeme denemesi,
- aynı cihazdan farklı kimliklerle çok sayıda sipariş,
- olağandışı yüksek değerli sipariş,
- teslimat adresinin sık değiştirilmesi,
- ödeme sonrasında hızlı adres değişikliği talebi,
- çok sayıda chargeback geçmişi,
- yeni hesap üzerinden olağandışı işlem hacmi,
- bilinen kötüye kullanım hesaplarıyla teknik bağlantı.

Bu göstergeler tek başına kötü niyetin kesin kanıtı değildir.

MADDE 28 - ÖDEME BAŞARISIZLIĞI

Ödeme işleminin başarısız olması halinde sipariş tamamlanmayabilir.

Kullanıcıya mümkün olduğu ölçüde;

- ödeme başarısız,
- tekrar deneyiniz,
- farklı ödeme yöntemi kullanınız

şeklinde açık bilgi verilir.

Kart reddinin bankadan kaynaklanan ayrıntılı nedeni Yedeknokta tarafından her zaman görüntülenemeyebilir.

MADDE 29 - MÜKERRER TAHSİLAT

Aynı sipariş için mükerrer tahsilat şüphesi oluşması halinde;

1. Platform kayıtları kontrol edilir.
2. Ödeme sağlayıcısı kayıtları kontrol edilir.
3. Banka/işlem kayıtları karşılaştırılır.
4. Fazla tahsilat doğrulanırsa gerekli iade işlemi gerçekleştirilir.

MADDE 30 - ÖDEME MUTABAKATI

Ödeme kayıtları;

- Platform,
- ödeme hizmeti sağlayıcısı,
- banka,
- Satıcı hakediş sistemi

arasında düzenli olarak mutabakata tabi tutulur.

MADDE 31 - MUTABAKATTA KONTROL EDİLECEK İŞLEMLER

Kontrolde özellikle;

- başarılı ödeme olup siparişe dönüşmeyen işlemler,
- sipariş olup ödeme kaydı bulunmayan işlemler,
- mükerrer tahsilatlar,
- iadesi sistemde tamamlanmamış işlemler,
- chargeback işlemleri,
- Satıcı hakedişiyle uyuşmayan kayıtlar

incelenir.

MADDE 32 - PARA İADESİ

Cayma, sipariş iptali, ayıplı ürün veya diğer hukuka uygun nedenlerle para iadesi gerektiğinde işlem, ilgili tüketici mevzuatı, Platform politikaları ve Satıcı/Mağaza Sözleşmesi doğrultusunda gerçekleştirilir. Satıcı adına bedel tahsil edilen işlemlerde Yedeknokta'nın iade sorumluluğu, yürürlükteki mevzuatta öngörülen hâl ve kapsamla sınırlıdır.

MADDE 33 - İADENİN ORJİNAL ÖDEME ARACINA YAPILMASI

Teknik ve hukuki olarak mümkün olduğu ölçüde para iadesi, ödemenin yapıldığı ödeme aracına gerçekleştirilir.

Örneğin kartla yapılan ödemenin nakit veya ilgisiz üçüncü kişinin banka hesabına iade edilmesinden kaçınılır.

Bu yaklaşım dolandırıcılık ve kara para aklama risklerinin azaltılmasına da yardımcı olur.

MADDE 34 - MANUEL İADE

Standart ödeme sağlayıcısı iade fonksiyonu dışında manuel para iadesi yapılması gerekiyorsa;

- iade sebebi,
- işlem numarası,
- tutar,
- ödeme alıcısı,
- onaylayan kişi

kayıt altına alınır.

MADDE 35 - ÜÇÜNCÜ KİŞİ HESABINA İADE

Para iadesinin siparişte kullanılan ödeme aracından farklı ve üçüncü kişiye ait hesaba yapılması talepleri yüksek riskli işlem olarak değerlendirilebilir.

Bu tür taleplerde ek doğrulama yapılmadan ödeme gerçekleştirilmemesi esastır.

MADDE 36 - KISMİ İADE

Bir siparişte yalnızca bazı ürünlerin iade edilmesi halinde kısmi para iadesi yapılabilir.

Kısmi iadede;

- ürün bedeli,
- indirim,
- kupon,
- kampanya,
- kargo bedeli

ilgili tüketici mevzuatı ve kampanya koşulları çerçevesinde değerlendirilir.

MADDE 37 - İADE KAYDI

Her para iadesinde mümkün olduğu ölçüde;

- sipariş numarası,
- ödeme işlem numarası,
- iade sebebi,
- iade tutarı,

- iade tarihi,
- ödeme sağlayıcısı işlem numarası,
- işlemi yapan/onaylayan

kayıt altına alınır.

MADDE 38 - BANKA TARAFINDAN İADENİN HESABA YANSITILMASI

Yedeknokta veya Satıcı tarafından ödeme sağlayıcısına iade talimatı verilmesi ile bankanın iadeyi kullanıcının kartına veya hesabına yansıtması farklı aşamalardır.

Kullanıcıya mümkün olduğu ölçüde iadenin işlem tarihi ve durumu hakkında bilgi sağlanır.

MADDE 39 - CHARGEBACK / TERS İBRAZ

Chargeback; kart sahibinin kart işlemi hakkında bankası veya ilgili ödeme sistemi nezdinde itirazda bulunması üzerine başlayan ters ibraz sürecini ifade eder.

Chargeback kararı yalnızca Yedeknokta tarafından verilen bir karar değildir; banka, ödeme hizmeti sağlayıcısı ve kart sistemi kuralları çerçevesinde yürütülebilir.

MADDE 40 - CHARGEBACK NEDENLERİ

Chargeback örneğin;

- işlem bana ait değil,
- ürün teslim edilmedi,
- işlem mükerrer,
- iade yapılmadı,
- ürün/hizmet açıklamaya uygun değil,
- sipariş iptal edildiği halde tahsilat yapıldı

gibi nedenlerle başlatılabilir.

MADDE 41 - CHARGEBACK BİLDİRİMİNİN ALINMASI

Ödeme sağlayıcısından chargeback bildirimi alındığında;

- işlem numarası,
- sipariş numarası,
- itiraz nedeni,
- cevap süresi,
- talep edilen belgeler

kayıt altına alınır.

MADDE 42 - CHARGEBACK DOSYASI

Her chargeback işlemi için mümkün olduğu ölçüde ayrı elektronik dosya oluşturulur.

Dosyada;

- sipariş bilgileri,
- ödeme kaydı,
- Satıcı bilgileri,
- ürün bilgileri,
- teslimat belgesi,
- kargo kaydı,
- kullanıcı yazışmaları,
- iade kayıtları,
- gerekli diğer deliller

tutulabilir.

MADDE 43 - CHARGEBACK SAVUNMASI

İtirazın haksız olduğu düşünülüyorsa, ödeme sağlayıcısının belirlediği süre içerisinde mevcut objektif belgeler sunulur.

Gerçekte bulunmayan;

- teslim belgesi,
- kullanıcı onayı,
- yazışma,
- fatura

oluşturulamaz veya gerçeğe aykırı şekilde değiştirilemez.

MADDE 44 - TESLİMAT İTİRAZLARI

“Ürün teslim edilmedi” gerekçeli chargeback işlemlerinde;

- kargo takip kaydı,
- teslim tarihi,
- teslim alan bilgisi,
- elektronik teslim belgesi,
- ilgili yazışmalar

incelenebilir.

MADDE 45 - YETKİSİZ İŞLEM İTİRAZLARI

“İşlem bana ait değil” itirazında;

- ödeme doğrulama yöntemi,
- 3D Secure kaydı - varsa,
- hesap giriş kayıtları,
- cihaz/IP bilgileri,
- sipariş ve teslimat bilgileri

hukuka uygun ve gerekli olduğu ölçüde incelenebilir.

MADDE 46 - İADE YAPILMADI İTİRAZI

Para iadesi yapıldığı halde chargeback başlatılmışsa;

- ödeme sağlayıcısının refund işlem numarası,
- iade tarihi,
- iade tutarı

dosyaya eklenir.

Aynı bedelin hem refund hem chargeback yoluyla iki kez kullanıcıya dönmesi ihtimali mutabakat sürecinde kontrol edilir.

MADDE 47 - CHARGEBACK SONUCU

Chargeback sonucu;

- kabul,
- itiraz kabul,
- itiraz reddi,
- kısmi kabul

şeklinde kayıt altına alınabilir.

MADDE 48 - CHARGEBACK MALİYETLERİ

Satıcının;

- ürünü göndermemesi,
- yanlış ürün göndermesi,
- iade yükümlülüğünü yerine getirmemesi,
- sahte ürün satması,

- kendi kusurundan kaynaklanan başka bir işlem

nedeniyle chargeback doğması veya Yedeknokta'nın bu nedenle ödeme hizmeti sağlayıcısı, banka, kart sistemi ya da Alıcıya ödeme yapmak, bedel iade etmek veya masraf üstlenmek zorunda kalması halinde, Satıcı/Mağaza Sözleşmesi hükümleri çerçevesinde ilgili tutar, chargeback ve işlem masrafları ile Yedeknokta'nın belgelendirilebilir doğrudan zararları Satıcı hakedişlerinden mahsup edilebilir; hakedişin yetersiz kalması halinde Satıcıya rücu edilebilir.

MADDE 49 - CHARGEBACK'İN OTOMATİK OLARAK SATICI KUSURU SAYILMAMASI

Her chargeback işlemi otomatik olarak Satıcının kusuru veya ihlali olarak kabul edilmez; ancak Satıcının teslim, iade, ürün uygunluğu, kartlı işlem güvenliği veya belge sunma yükümlülüğünü ihlal ettiğinin makul kayıt ve belgelerle tespit edildiği haller saklıdır.

İşlem;

- chargeback nedeni,
- mevcut deliller,
- teslimat,
- kullanıcı davranışı,
- Satıcının açıklaması

birlikte değerlendirilerek sonuçlandırılır.

MADDE 50 - CHARGEBACK PERFORMANS TAKİBİ

Satıcı bazında;

- chargeback sayısı,
- chargeback oranı,
- chargeback nedenleri,
- kaybedilen itiraz oranı

izlenebilir.

Olağandışı yüksek chargeback oranı ek inceleme veya Satıcı performans tedbiri sebebi olabilir.

MADDE 51 - SATICI HAKEDİŞLERİ

Satıcı satışlarından doğan hakedişler Satıcı/Mağaza Sözleşmesinde belirlenen;

- komisyon,

- iade,
- iptal,
- chargeback,
- diğerk hukuka uygun kesintiler

dikkate alınarak hesaplanır. Hakedişler, Satıcı/Mağaza Sözleşmesinde belirlenen ödeme takvimi, doğrulama, mutabakat, iade ve chargeback süreçleri tamamlandıktan sonra Satıcının doğrulanmış hesabına aktarılır.

MADDE 52 - SATICI ÖDEME HESABI

Satıcı hakedişi mümkün olduğu ölçüde Satıcının doğrulanmış banka hesabına aktarılır.

Banka hesabında yapılan değişikliklerde tekrar doğrulama uygulanabilir; doğrulama tamamlanıncaya kadar hakediş ödemesi geçici olarak bekletilebilir.

MADDE 53 - SATICI BANKA HESABI DEĞİŞİKLİĞİ

Banka hesabı değişiklikleri yüksek riskli işlem olarak değerlendirilebilir.

Değişiklikte;

- hesap doğrulaması,
- yetkili kişi kontrolü,
- MFA,
- ikinci onay,
- değişiklik bildirimi

uygulanabilir.

MADDE 54 - HAKEDİŞİN GEÇİCİ İNCELEMeye ALINMASI

Güçlü;

- dolandırıcılık,
- hesap ele geçirilmesi,
- sahte ürün,
- yoğun chargeback,
- ödeme manipölasyonu

şüphesi halinde ilgili hakediş, Satıcı/Mağaza Sözleşmesi ve yürürlükteki mevzuata uygun olarak, güvenlik incelemesi ve gerekli bilgi-belgelerin temini sonuçlanıncaya kadar gerekli ve ölçülü süreyle geçici incelemeye alınabilir. Yedeknokta, mümkün olduğu ölçüde Satıcıyı

incelemenin nedeni ve talep edilen bilgi-belgeler hakkında dâhili iletişim sistemi üzerinden bilgilendirir.

Belirsiz ve süresiz ödeme bloke uygulamasından kaçınılır.

MADDE 55 - SİBER GÜVENLİK OLAYI

Ödeme altyapısında;

- yetkisiz erişim,
- kart verisi sızıntısı,
- ödeme panelinin ele geçirilmesi,
- API anahtarı sızıntısı,
- sahte ödeme sayfası,
- zararlı yazılım

gibi olaylar kritik güvenlik olayı olarak değerlendirilir.

MADDE 56 - ÖDEME GÜVENLİĞİ OLAYINDA İLK İŞLEMLER

Olay tespit edildiğinde;

1. Etkilenen sistem belirlenir.
2. Gerekirse ödeme işlemleri geçici olarak sınırlandırılır.
3. Yetkisiz erişim engellenir.
4. Kritik erişim anahtarları değiştirilir.
5. Ödeme sağlayıcısı bilgilendirilir.
6. Log ve deliller korunur.
7. Kişisel veri ihlali değerlendirmesi yapılır.
8. Gerekli hukuki bildirimler değerlendirilir.

MADDE 57 - API VE ANAHTAR GÜVENLİĞİ

Ödeme sağlayıcılarına ait;

- API anahtarları,
- secret key'ler,
- sertifikalar,
- erişim tokenları

kaynak kod içerisinde açık şekilde saklanmamalıdır.

Bu bilgiler güvenli sır yönetim sistemlerinde tutulur ve erişimleri sınırlandırılır.

MADDE 58 - TEST VE ÜRETİM ORTAMLARI

Ödeme sağlayıcısının test/sandbox bilgileri ile üretim bilgileri birbirinden ayrılır.

Test ortamında gerçek kart bilgilerinin gereksiz şekilde kullanılmaması esastır.

MADDE 59 - WEBHOOK / CALLBACK GÜVENLİĞİ

Ödeme sağlayıcısından gelen ödeme sonucu bildirimlerinin;

- kaynağının doğrulanması,
- imza/token kontrolü,
- tekrarlanan bildirimlerin yönetilmesi,
- sahte callback taleplerinin engellenmesi

için teknik kontroller uygulanır.

MADDE 60 - MÜKERRER İŞLEM ÖNLEME

Teknik sistem mümkün olduğu ölçüde;

- aynı ödeme talebinin birden fazla işlenmesini,
- sayfa yenileme nedeniyle çift tahsilatı,
- webhook tekrarları nedeniyle mükerrer kayıt oluşmasını

engelleyecek idempotency veya benzeri kontroller içermelidir.

MADDE 61 - ÖDEME SAYFASI DEĞİŞİKLİKLERİ

Ödeme ekranı veya ödeme entegrasyonunda önemli değişiklik yapılmadan önce;

- bilgi güvenliği,
- kullanıcı deneyimi,
- KVKK,
- ödeme mevzuatı,
- fraud etkisi

değerlendirilebilir.

MADDE 62 - ÖDEME SAĞLAYICISI KESİNTİSİ

Ödeme sağlayıcısında hizmet kesintisi halinde;

- yeni ödeme alınması geçici olarak durdurulabilir,
- kullanıcıya hata mesajı gösterilebilir,

- alternatif sağlayıcı varsa devreye alınabilir,
- belirsiz işlem durumları sonradan mutabakata tabi tutulur.

MADDE 63 - BELİRSİZ ÖDEME DURUMU

Kullanıcının hesabından tahsilat yapılmış görünmesine rağmen Platform'un ödeme sonucunu alamaması halinde sipariş otomatik olarak ikinci kez tahsil edilmeye çalışılmaz.

Önce ödeme sağlayıcısının işlem durumu doğrulanır.

MADDE 64 - KİŞİSEL VERİLER

Ödeme işlemleri kapsamında;

- ödeme işlem bilgileri,
- banka/IBAN bilgileri,
- IP ve cihaz bilgileri,
- fraud kayıtları

gibi kişisel veriler işlenebilir.

Bu veriler; ödeme işlemlerinin yürütülmesi, iade ve chargeback süreçlerinin yönetimi, dolandırıcılığın önlenmesi, uyuşmazlıkların çözümü, hukuki yükümlülüklerin yerine getirilmesi ve Yedeknokta'nın haklarının tesisi, kullanılması veya korunması amaçlarıyla, ilgili aydınlatma yükümlülükleri yerine getirilerek ve uygun hukuki sebebe dayanılarak işlenir.

MADDE 65 - FRAUD VERİLERİNİN SAKLANMASI

Dolandırıcılık önleme amacıyla oluşturulan;

- risk puanları,
- kara liste kayıtları,
- cihaz bağlantıları,
- şüpheli işlem işaretleri

gereksiz veya süresiz biçimde saklanmamalıdır.

Saklama süresi veri işleme amacı ve hukuki dayanakla uyumlu şekilde belirlenir.

MADDE 66 - KARA LİSTE UYGULAMALARI

Kötüye kullanımın önlenmesi amacıyla iç risk listeleri oluşturulması halinde;

- objektif gerekçe,
- güncellik,

- yanlış pozitiflerin düzeltilmesi,
- erişim sınırları

sağlanır.

Kişilerin keyfî veya doğrulanmamış iddialarla kalıcı olarak kara listeye alınmasından kaçınılır.

MADDE 67 - MASAK / AML SÜREÇLERİYLE İLİŞKİ

Ödeme ve fraud kontrolleri, Yedeknokta'nın hukuken tabi olması halinde uygulanacak AML/KYC veya diğer mali suçların önlenmesine ilişkin yükümlülüklerin yerine geçmez; Yedeknokta'nın bu yükümlülüklere tabi olmaması halinde dahi, ödeme hizmeti sağlayıcısının veya yetkili makamların mevzuata uygun bilgi ve belge talepleri ilgili süreçler çerçevesinde değerlendirilir.

Bu konular ayrıca AML/KYC/Yaptırım ve Şüpheli İşlem Politikası kapsamında değerlendirilir.

MADDE 68 - ÖDEME UYUŞMAZLIKLARINDA DELİLLER

Ödeme uyumsuzluklarında;

- ödeme sağlayıcı kayıtları,
- sipariş kayıtları,
- teslimat kayıtları,
- sistem logları,
- kullanıcı yazışmaları

hukuka uygun şekilde, bütünlüğü ve erişilebilirliği korunarak muhafaza edilir; Satıcı, talep edilen bilgi ve belgeleri Satıcı/Mağaza Sözleşmesinde öngörülen sürelerde Yedeknokta'ya sunmakla yükümlüdür.

Kayıtlar gerçeğe aykırı şekilde değiştirilemez.

MADDE 69 - LOG YÖNETİMİ

Ödeme işlemlerinde mümkün olduğu ölçüde;

- işlem kimliği,
- tarih/saat,
- işlem durumu,
- iade durumu,
- işlem yapan kullanıcı,
- sistem sonucu

loglanır.

Loglarda tam kart numarası, CVV veya diğer gereksiz hassas ödeme verilerinin tutulmaması esastır.

MADDE 70 - DENETİM

Ödeme süreçleri periyodik olarak denetlenebilir.

Denetimde özellikle;

- kullanıcı yetkileri,
- kart verisi işleme,
- PCI kapsamı,
- ödeme sağlayıcıları,
- refund işlemleri,
- chargeback kayıtları,
- Satıcı hakedişleri,
- banka hesabı değişiklikleri,
- fraud kuralları

incelenir.

MADDE 71 - ÖDEME GÜVENLİĞİ KONTROL LİSTESİ

- Aktif ödeme sağlayıcıları kayıtlı.
- Sağlayıcı sözleşmeleri güncel.
- Kart verisinin sistemden geçip geçmediği biliniyor.
- CVV/CVC saklanmıyor.
- Tokenizasyon kullanımı değerlendirildi.
- PCI DSS kapsamı değerlendirildi.
- Ödeme panelinde MFA aktif.
- Admin erişimleri sınırlı.
- Fraud kuralları mevcut.
- Yüksek riskli işlemler için manuel inceleme var.
- Mükerrer tahsilat kontrolleri mevcut.
- Refund kayıtları izlenebilir.
- Chargeback dosyaları tutuluyor.
- Satıcı ödeme hesapları doğrulanıyor.
- Banka hesabı değişiklikleri ayrıca kontrol ediliyor.

- Ödeme sağlayıcı mutabakatı yapılıyor.
- Ödeme loglarında hassas kart verisi bulunmuyor.
- API anahtarları güvenli saklanıyor.
- Ödeme güvenliği olay müdahale süreci biliniyor.

MADDE 72 - REFUND KONTROL FORMU

Sipariş No: [●]

Ödeme İşlem No: [●]

Kullanıcı: [●]

Satıcı: [●]

Ödeme Tutarı: [●]

İade Tutarı: [●]

İade Sebebi: [●]

İade Türü: Tam / Kısmi

Orijinal Ödeme Aracına mı?: Evet / Hayır

Manuel İşlem mi?: Evet / Hayır

İade Tarihi: [●]

Sağlayıcı Refund No: [●]

İşlemi Yapan: [●]

Onaylayan: [●]

MADDE 73 - CHARGEBACK KONTROL FORMU

Dosya No: [●]

Bildirim Tarihi: [●]

Ödeme Sağlayıcısı: [●]

Sipariş No: [●]

İşlem No: [●]

Tutar: [●]

Chargeback Nedeni: [●]

Cevap Son Tarihi: [●]

Satıcı Bilgilendirildi mi?: [●]

Teslimat Delili: [●]

Ödeme Doğrulama Kaydı: [●]

Kullanıcı Yazışmaları: [●]

Refund Var mı?: [●]

Savunma Sunuldu mu?: [●]

Sonuç: [●]

Satıcı Kusuru Tespit Edildi mi?: [●]

Mahsup/Rücu Gerekiyor mu?: [●]

Dosyanın Kapanış Tarihi: [●]

MADDE 74 - FRAUD İNCELEME FORMU

İşlem No: [●]

Sipariş No: [●]

Tespit Tarihi: [●]

Risk Seviyesi: Düşük / Orta / Yüksek

Risk Göstergeleri: [●]

Otomatik Sistem Skoru: [●]

Manuel İnceleme Yapıldı mı?: [●]

Ek Doğrulama: [●]

Sonuç:

- İşlem devam
- Ek doğrulama
- Geçici bekletme
- İptal
- Güvenlik olayına eskalasyon

Kararı Veren: [●]

Gerekçe: [●]

MADDE 75 - POLİTİKANIN GÖZDEN GEÇİRİLMESİ

İşbu Politika en az [YILLIK] olarak ve ayrıca;

- yeni ödeme sağlayıcısı,
- yeni sanal POS,
- ödeme mimarisi değişikliği,
- önemli fraud olayı,
- kart verisi güvenliği olayı,
- mevzuat değişikliği

halinde gözden geçirilir.

MADDE 76 - YÜRÜRLÜK

İşbu Ödeme, İşlem Güvenliği ve İade/Chargeback Politikası [●] tarihinde yürürlüğe girer.

Doküman Sahibi: [●]

Onaylayan: [●]

Versiyon: 1.0

Yürürlük Tarihi: [●]

Son Gözden Geçirme Tarihi: [●]