



BİLGİ GÜVENLİĞİ POLİTİKASI

DOKÜMAN NO	BT.PO.000
REVİZYON NO	01
YAYIN TARİHİ	07.08.2024
REVİZYON TARİHİ	30.09.2026
ONAY MERCİİ	Yönetim Kurulu

Alan	Bilgi	Alan	Bilgi
Doküman Adı	Bilgi Sistemleri Yönetimi ve Bilgi Güvenliği Politikası	Doküman Kodu	BT.PO.000
Sahip Birim	Bilgi Güvenliği Müdürlüğü	İlgili Birimler	BT, Hukuk, Sermaye Piyasaları Uyum, İç Denetim, İnsan Kaynakları, Süreç Sahipleri
Yürürlük	Yönetim Kurulu onayı sonrası	Gözden Geçirme	En az yılda bir veya önemli değişikliklerde
Sınıflandırma	Genel	Kapsam	Koton bilgi sistemleri, bilgi varlıkları, çalışanlar ve üçüncü taraflar
Onay	Yönetim Kurulu	Versiyon	Rev.01

İÇİNDEKİLER

1. AMAÇ VE KAPSAM
2. YASAL DAYANAK VE REFERANSLAR
3. TANIMLAR
4. GENEL İLKELER
5. BİLGİ SİSTEMLERİ YÖNETİMİ
6. BİLGİ GÜVENLİĞİ YÖNETİMİ
7. BİLGİ SİSTEMLERİ RİSK YÖNETİMİ
8. BİLGİ SİSTEMLERİ SÜREKLİLİK YÖNETİMİ
9. ROLLER VE SORUMLULUKLAR
10. ÜÇÜNCÜ TARAFLAR VE DIŞ HİZMET ALIMLARI
11. UYUM, GÖZETİM VE İHLAL YÖNETİMİ
12. EĞİTİM VE FARKINDALIK
13. POLİTİKANIN GÖZDEN GEÇİRİLMESİ VE GÜNCELLENMESİ
14. HEDEFLER
15. YÜRÜRLÜK VE ONAY

1. AMAÇ VE KAPSAM

Bu politikanın amacı; Koton Mağazacılık Tekstil Sanayi ve Ticaret A.Ş. bünyesinde kullanılan bilgi sistemlerinin, bilgi varlıklarının ve bu varlıklarla ilişkili süreçlerin gizlilik, bütünlük ve erişilebilirliğini korumak; bilgi sistemleri yönetimi, bilgi güvenliği, bilgi sistemleri risk yönetimi ve bilgi sistemleri süreklilik yönetimine ilişkin temel ilkeleri belirlemektir.

Politika; Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği'nin halka açık ortaklıklara yönelik yükümlülükleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili diğer mevzuat dikkate alınarak hazırlanmıştır.

Bu politika; tam zamanlı, yarı zamanlı, dönemsel veya sözleşmeli çalışanlar, stajyerler, danışmanlar, tedarikçiler, dış hizmet sağlayıcıları, iş ortakları ve Koton bilgi sistemlerine veya bilgi varlıklarına erişen tüm üçüncü taraflar için geçerlidir. Coğrafi konum, iş birimi, iş modeli veya çalışma şekli kapsamı daraltmaz.

Koton, bilgi sistemleri yönetimine ilişkin kontrolleri tesis etmeyi, yazılı politika, prosedür, standart, talimat ve süreçlerle desteklemeyi, düzenli olarak gözden geçirmeyi, teknolojik gelişmeler ve iş süreçlerindeki değişiklikler doğrultusunda güncellemeyi taahhüt eder.

2. YASAL DAYANAK VE REFERANSLAR

- Sermaye Piyasası Kurulu VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil düzenlemeler.
- 6102 sayılı Türk Ticaret Kanunu ve ilgili sermaye piyasası mevzuatı.
- 5651 sayılı Kanun ve bilgi sistemleri kayıtlarının tutulmasına ilişkin yükümlülükler.
- ISO/IEC 27001: 2022 Bilgi Güvenliği Yönetim Sistemi standardı ve ilgili iyi uygulama rehberleri.
- ISO 22301 İş Sürekliliği Yönetim Sistemi standardı ve Koton iş sürekliliği süreçleri.
- Koton iç politika, prosedür, standart, talimat, sözleşme, taahhütname ve veri koruma dokümanları.

3. TANIMLAR

Terim	Açıklama
Bilgi Sistemleri	Bilginin işlendiği, iletildiği ve saklandığı yazılım, donanım, iletişim altyapısı, insan kaynağı, faaliyet ve süreçlerin bütünü.
Bilgi Varlığı	Koton faaliyetleri kapsamında üretilen, işlenen, iletilen veya saklanan veri ile bu verilerin bulunduğu sistem, uygulama, donanım ve ortamlar.
Bilgi Güvenliği	Bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilirliğinin korunmasına yönelik idari, teknik ve fiziksel tedbirlerin bütünü.
Bilgi Güvenliği İhlali	Bilgi sistemlerinin veya bilgilerin gizlilik, bütünlük ya da erişilebilirliğini ihlal eden veya ihlal etmeye teşebbüs eden olaylar.
Üst Yönetim	Koton'da Genel Müdür ile bilgi sistemleri ve bilgi güvenliği yönetiminden sorumlu ilgili Grup Direktörü.
Bilgi Güvenliği Sorumlusu	Yönetim Kurulu tarafından Üst Yönetim'e bağlı olarak görevlendirilen; bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesini ve takibini, risklerin izlenmesini ve üst yönetime raporlanmasını gözetan sorumlu rol.
Varlık/Süreç Sahibi	Bilgi varlığının veya iş sürecinin iş gereksinimleri, erişim ihtiyaçları, riskleri ve sınıflandırmasından sorumlu kişi veya birim.

4. GENEL İLKELER

Koton, bilgi sistemleri yönetimini kurumsal yönetim uygulamalarının ayrılmaz bir parçası olarak ele alır. Bilgi sistemleri stratejileri, iş hedefleri, risk iştahı, mevzuat gereklilikleri, müşteri ve paydaş beklentileri ile uyumlu şekilde yönetir.

- Bilgi varlıkları iş değeri, kritiklik seviyesi, gizlilik, bütünlük ve erişilebilirlik ihtiyaçları doğrultusunda korunur.
- Bilgi sistemleri yönetiminde görevler ayrılığı, en az yetki, ihtiyaç kadar erişim, izlenebilirlik ve hesap verebilirlik ilkeleri uygulanır.
- Bilgi güvenliği riskleri sistematik olarak belirlenir, değerlendirilir, işlenir, izlenir ve üst yönetime raporlanır.
- Bilgi sistemleri sürekliliği; iş sürekliliği, felaket kurtarma, yedekleme, kriz yönetimi ve test/tatbikat faaliyetleriyle desteklenir.
- Kişisel veriler, ticari sırlar, finansal bilgiler, müşteri ve çalışan bilgileri ilgili mevzuat ve Koton iç düzenlemelerine uygun korunur.
- Politika gerekleri, alt politika, prosedür, standart, talimat, kontrol listesi ve teknik kontrollerle desteklenir.
- Politika ve bağlı dokümanlar, çalışanlara ve ilgili taraflara duyurulur; uyumun sağlanması için farkındalık faaliyetleri yürütülür.

5. BİLGİ SİSTEMLERİ YÖNETİMİ

Koton, bilgi sistemlerinin kurulması, işletilmesi, kullanılması, izlenmesi, değiştirilmesi, devreden çıkarılması ve üçüncü taraflarla ilişkili süreçlerini kontrollü ve dokümente edilmiş şekilde yönetir.

5.1 YÖNETİŞİM VE YÖNETİM YAPISI

- Yönetim Kurulu, bilgi sistemleri yönetimi ve bilgi güvenliği politikasını onaylar; etkin bir yönetim yapısının tesis edilmesini gözetir.
- Üst Yönetim, bilgi güvenliği politikasını hazırlar, bilgi sistemleri yönetimi için gerekli kaynak, rol, sorumluluk ve yetkilerin tahsis edilmesini sağlar.
- Bilgi Güvenliği Sorumlusu, bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumludur. Bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime rapor verir. Bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye ve en az 5 yıl tecrübeye sahip kişiler içinden belirlenir. Bilgi güvenliği sorumlusunun, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevi bulunmaz. Görevlerini bağımsız şekilde yürütür ve doğrudan Üst Yönetime bağlı çalışır.
- Bilgi teknolojileri, bilgi güvenliği, hukuk, sermaye piyasaları uyum, iç denetim, insan kaynakları ve süreç sahipleri, politika gerekliliklerinin kendi sorumluluk alanlarında uygulanmasına katkı sağlar.

5.2 POLİTİKA, PROSEDÜR VE KONTROLLER

- Bilgi sistemleri yönetimine ilişkin politika, prosedür, standart, talimat ve süreçler yazılı hale getirilir.
- Kontroller; erişim yönetimi, kimlik doğrulama, log yönetimi, değişiklik yönetimi, güvenli yazılım geliştirme, yedekleme, tedarikçi güvenliği ve olay yönetimi gibi alanları kapsayacak şekilde uygulanır.
- Kontrollerin etkinliği düzenli olarak izlenir, ölçülür ve iyileştirilir. Kontrol etkinliği; güvenlik olayı sayısı, risk seviyesi, kritik zafiyet kapatma süresi, erişim gözden geçirme tamamlanma oranı, eğitim katılım oranı, olay müdahale süresi, süreklilik test sonuçları ve üçüncü taraf güvenlik bulguları gibi ölçülebilir göstergelerle değerlendirilir. Önemli kontrol eksiklikleri ve iyileştirme çalışmaları üst yönetime raporlanır.
- İş alanında gerçekleşen değişiklikler, mevzuat güncellemeleri, teknolojik gelişmeler ve tehdit ortamındaki değişimler doğrultusunda dokümanlar güncellenir.

5.3 GÖREVLER AYRILIĞI VE YETKİLENDİRME

- Kritik bilgi sistemleri süreçlerinde görevler ayrılığı ilkesi uygulanır.
- Erişim hakları kullanıcının iş ihtiyacı, rolü ve yetki seviyesiyle sınırlı olacak şekilde tanımlanır.
- Ayrıcalıklı hesaplar ve kritik işlemler izlenir, kayıt altına alınır ve periyodik olarak gözden geçirilir.
- Geçici veya acil erişimler kontrollü, süreli, onaylı ve izlenebilir şekilde yürütülür.

6. BİLGİ GÜVENLİĞİ YÖNETİMİ

Koton, bilgi güvenliğini yalnızca teknik kontrollerle sınırlı görmez; insan, süreç, teknoloji ve üçüncü taraf boyutlarını kapsayan bütünlüklü bir yönetim sistemi olarak ele alır.

- Gizlilik: Bilgiye yalnızca yetkili kişi, sistem ve tarafların erişmesi sağlanır.
- Bütünlük: Bilginin doğruluğu, tamlığı ve yetkisiz değişikliklere karşı korunması sağlanır.
- Erişilebilirlik: Yetkili kullanıcıların, ihtiyaç duyulan bilgi ve sistemlere gerekli zamanda erişebilmesi hedeflenir.
- İzlenebilirlik: Kritik sistem, uygulama ve kullanıcı faaliyetleri uygun düzeyde kayıt altına alınır.
- Farkındalık: Çalışanların ve ilgili tarafların bilgi güvenliği sorumlulukları konusunda bilinçli hareket etmesi sağlanır.
- Olay Müdahalesi: Bilgi güvenliği ihlalleri hızlı şekilde tespit edilir, değerlendirilir, müdahale edilir, raporlanır ve iyileştirme fırsatına dönüştürülür.

7. BİLGİ SİSTEMLERİ RİSK YÖNETİMİ

Koton, bilgi sistemleri risklerini iş hedefleri, mevzuat yükümlülükleri, bilgi varlıklarının değeri, tehditler, zafiyetler ve mevcut kontroller dikkate alınarak yönetir.

- Bilgi varlıkları ve bağlı süreçler belirlenir, sahiplikleri tanımlanır ve envanterleri güncel tutulur.
- Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ihtiyaçları değerlendirilir.
- Tehdit ve zafiyetler belirlenir; gerçekleşme olasılığı ve olası etkiler analiz edilir.
- Riskler kabul, azaltma, aktarma veya kaçınma kararları doğrultusunda işlenir.
- Risk işleme planları için sorumlu, süre, hedef kontrol ve takip mekanizması belirlenir.
- Kabul edilen artık riskler uygun yetki seviyesinde onaylanır.
- Önemli bilgi güvenliği ve bilgi sistemleri riskleri periyodik olarak üst yönetime raporlanır.
- Yeni sistem, süreç, teknoloji, dış hizmet, entegrasyon veya önemli değişikliklerde risk değerlendirmesi yapılır.

8. BİLGİ SİSTEMLERİ SÜREKLİLİK YÖNETİMİ

Koton, bilgi sistemleri sürekliliğini iş sürekliliği yönetiminin temel unsurlarından biri olarak ele alır. Kritik iş süreçlerinin kesinti durumlarında kabul edilebilir süre ve veri kaybı hedefleri doğrultusunda sürdürülebilmesi amaçlanır.

- Kritik bilgi sistemleri, uygulamalar, altyapılar ve bağımlılıklar belirlenir.
- İş etki analizi sonuçları dikkate alınarak kurtarma öncelikleri, azami kesinti süreleri ve kabul edilebilir veri kaybı hedefleri tanımlanır.
- Yedekleme, felaket kurtarma, yüksek erişilebilirlik, alternatif lokasyon, iletişim ve kriz yönetimi stratejileri oluşturulur.
- İş sürekliliği ve felaket kurtarma planları düzenli olarak test edilir, tatbikat sonuçlarına göre iyileştirilir.
- Kritik sistemlerin sürekliliğini etkileyebilecek olaylar kayıt altına alınır, kök nedenleri analiz edilir ve tekrarını önleyici aksiyonlar planlanır.
- Dış hizmet sağlayıcılarının süreklilik yetkinlikleri, sözleşme ve hizmet seviyesi gereklilikleri kapsamında takip edilir.

9. ROLLER VE SORUMLULUKLAR

Rol / Taraf	Temel Sorumluluklar
Yönetim Kurulu	Politikayı onaylar, bilgi sistemleri yönetimi ve bilgi güvenliği yönetişiminin etkin şekilde kurulmasını ve uygulanmasını

	gözetir. Gereken durumlarda politika kapsamındaki yetkilendirmeleri yapar. Bilgi sistemlerinden kaynaklanan riskleri dikkate alarak stratejik kararlar alır. Bilgi Güvenliği Sorumlusu'nu belirler.
Üst Yönetim	Politikayı hazırlar, uygulanması için gerekli kaynak, yetki ve sorumlulukları sağlar. Bilgi sistemleri stratejilerinin iş hedefleriyle uyumlu yürütülmesini, risklerin ve önemli güvenlik konularının değerlendirilmesini sağlar. Bilgi Güvenliği Sorumlusu, kendisine bağlı çalışır.
Bilgi Güvenliği Sorumlusu	Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumludur. Bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime rapor verir. Görevlerini bağımsız şekilde yürütür ve doğrudan Üst Yönetime bağlı çalışır.
Bilgi Teknolojileri Operasyon Birimleri	Bilgi sistemleri altyapısı, erişim yönetimi, log yönetimi, güvenlik izleme, zafiyet yönetimi, olay müdahale, yedekleme ve süreklilik kontrollerinin uygulanmasını sağlar. Bilgi güvenliği gerekliliklerinin uygulanması, izlenmesi ve raporlanmasına yönelik faaliyetlerin yürütülmesini sağlar.
Varlık ve Süreç Sahipleri	Sahibi oldukları bilgi varlıklarının envanter, sınıflandırma, erişim, risk ve süreklilik ihtiyaçlarını belirler; süreç dokümanlarının bilgi güvenliği gereklilikleriyle uyumlu olmasını sağlar; risk değerlendirme çalışmalarına ve ilgili risk kabul kararlarına katkı sağlar.
Tüm Çalışanlar	Koton politika, prosedür ve talimatlarına uyar; bilgi güvenliği ihlali veya şüphesini ilgili kanallara bildirir; yalnızca iş gereği erişim talep eder ve kendisine tahsis edilen erişimleri sorumlu şekilde kullanır.
Üçüncü Taraflar	Sözleşmeler, gizlilik yükümlülükleri, güvenlik protokolleri ve Koton politika/prosedürlerine uygun hareket eder; Koton bilgilerini yetkisiz kişilerle paylaşmaz ve erişim değişikliklerini zamanında bildirir.

10. ÜÇÜNCÜ TARAFLAR VE DIŞ HİZMET ALIMLARI

Koton'a mal veya hizmet sağlayan üçüncü tarafların ve bu tarafların çalışanlarının bilgi güvenliği yükümlülükleri; sözleşmeler, gizlilik taahhütleri, servis seviyesi düzenlemeleri, güvenlik protokolleri ve ilgili Koton politika/prosedürleriyle belirlenir.

- Üçüncü taraflar, Koton'a ait bilgi ve varlıkları Koton'un yazılı onayı olmadan paylaşamaz, kopyalayamaz veya amacı dışında kullanamaz.

- Koton bilgi sistemlerine erişen üçüncü taraf kullanıcıların kimlikleri, yetkileri ve erişim süreleri kontrollü şekilde yönetilir.
- Üçüncü taraf çalışanlarının görev değişikliği veya işten ayrılması durumunda erişimlerin zamanında kapatılması için gerekli bildirimler yapılır.
- Dış hizmet sağlayıcılarının bilgi güvenliği, süreklilik, mevzuat uyumu ve log/denetim izi gerekliliklerine uygunluğu takip edilir.
- Kritik dış hizmetlerde hizmet seviyesi, erişilebilirlik, yedekleme, veri işleme, lokasyon, alt yüklenici, denetim ve olay bildirimi koşulları sözleşmelerde düzenlenir.

11. UYUM, GÖZETİM VE İHLAL YÖNETİMİ

Politika'nın kendi faaliyet alanlarına göre uygulanmasından ve Politika ve bağlı dokümanlara uyumun sağlanmasından Bilgi Güvenliği Müdürlüğü, ilgili birim yöneticileri, süreç sahipleri sorumludur; Bilgi Güvenliği Sorumlusu kontrollerin etkinliğini gözetir ve riskleri üst yönetime raporlar.

- Bilgi güvenliği ve bilgi sistemleri kontrollerinin etkinliği periyodik olarak izlenir, ölçülür ve raporlanır.
- Tebliğ kapsamındaki muafiyetler saklı kalmak kaydıyla, gerekli görülen alanlarda uyum, bağımsız değerlendirme veya denetim faaliyetleri yürütülür.
- Politika ihlalleri, ilgili iç düzenlemeler ve mevzuat hükümleri çerçevesinde değerlendirilir.
- İhlaller; disiplin süreci, erişim kısıtlama, sözleşmesel yaptırım, hukuki süreç veya düzeltici/önleyici faaliyetlerle sonuçlanabilir.
- İhlal ve olaylardan çıkarılan dersler, kontrollerin ve farkındalık faaliyetlerinin iyileştirilmesinde kullanılır.

12. EĞİTİM VE FARKINDALIK

Koton, bilgi güvenliği kültürünün geliştirilmesi amacıyla çalışanlara, süreç sahiplerine, kritik rol sahiplerine ve gerekli görülen üçüncü taraflara uygun farkındalık ve eğitim faaliyetleri sağlar.

- Yeni başlayan çalışanlara temel bilgi güvenliği ve veri koruma farkındalığı kazandırılır.
- Düzenli farkındalık eğitimleri, duyurular, simülasyonlar ve bilgilendirmelerle güvenli davranış alışkanlıkları desteklenir.
- Tüm çalışanlara bilgi güvenliği gereklilikleri, güncel tehditler, riskler ve ihlal bildirimi konusunda yılda en az bir kez farkındalık eğitimi verilir.
- Ayrıcalıklı erişime sahip kullanıcılar, süreç ve varlık sahipleri ile teknik ekipler için rol bazlı eğitimler planlanır.
- Eğitim katılımı ve farkındalık sonuçları takip edilerek iyileştirme alanları belirlenir.

13. POLİTİKANIN GÖZDEN GEÇİRİLMESİ VE GÜNCELLENMESİ

Bu politika en az yılda bir kez veya aşağıdaki durumlardan herhangi biri gerçekleştiğinde gözden geçirilir:

- SPK, KVKK veya ilgili diğer mevzuatta önemli değişiklik olması.
- Koton'un iş modeli, organizasyon yapısı, teknoloji kullanımı veya kritik süreçlerinde önemli değişiklik olması.
- Önemli bilgi güvenliği olayı, denetim bulgusu, risk artışı veya kontrol zafiyeti tespit edilmesi.
- Yeni sistem, hizmet, dış kaynak kullanımı veya kritik entegrasyonların devreye alınması.
- Tehdit ortamında veya teknolojik gelişmelerde politika kapsamını etkileyen önemli değişiklikler yaşanması.

Güncellemeler, Bilgi Güvenliği Müdürlüğü koordinasyonunda ilgili paydaşların görüşleri alınarak hazırlanır ve gerekli onay süreçleri tamamlandıktan sonra yürürlüğe alınır.

14. HEDEFLER

Koton, bilgi sistemleri yönetimi ve bilgi güvenliği kapsamında aşağıdaki hedefleri benimser:

- Bilgi sistemlerinin sürekliliğini, erişilebilirliğini ve güvenilirliğini iş ihtiyaçlarıyla uyumlu şekilde sağlamak.
- Bilgi güvenliği risklerini kabul edilebilir seviyede tutmak ve risk yönetimini sürekli iyileştirmek.
- Yasal, düzenleyici ve sözleşmesel yükümlülüklerle uyum sağlamak.
- Bilgi güvenliği olaylarını önlemek, erken tespit etmek, hızlı müdahale etmek ve etkilerini azaltmak.
- Çalışanların ve ilgili tarafların bilgi güvenliği farkındalık ve uyum düzeyini artırmak.
- Kritik bilgi sistemleri için süreklilik, yedekleme ve felaket kurtarma yetkinliklerini güçlendirmek.
- Üçüncü taraflarla yürütülen süreçlerde bilgi güvenliği ve veri koruma gerekliliklerine uyumu sağlamak.
- Bilgi güvenliği yönetim sistemi ve ilgili kontrollerin etkinliğini düzenli olarak izlemek, ölçmek ve iyileştirmek.

15. YÜRÜRLÜK VE ONAY

Bu Politika, Yönetim Kurulu onayıyla yürürlüğe girer. Politikada yapılacak değişiklikler de Yönetim Kurulu onayına tabidir. Söz konusu politikanın isleyişi düzenli olarak gözden geçirilir ve gereksinimler doğrultusunda güncellenerek güncel politika metni çalışanlara ve ilgili paydaşlara duyurulur. Politikanın uygulanmasını ve yükümlülüklerin yerine getirilmesini Üst Yönetim gözetir. Politika kapsamında bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu

bir şekilde tesis edilmesi, deęerlendirilmesi ve gözetimi Yönetim Kurulu'nun sorumluluęundadır.

SPK VII-128.10 sayılı Teblię'in "Muafiyetler" başlıklı 30'uncu maddesi kapsamında halka açık ortaklıklar için uygulanması zorunlu olmayan madde ve fıkralar saklıdır. Bu politika ve baęlı dokümanlar, Koton'un halka açık ortaklık sıfatı kapsamında tabi olduęu yükümlölükler dikkate alınarak uygulanır.