ALLBATROSS YATIRIM MENKUL DEĞERLER A.Ş.

Kişisel Veri Saklama ve İmha Politikası

Doküman Adı	**KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**
Doküman No	**ALQ-PO-013**
Versiyon Tarihi ve No	**07.11.2024-01**
Gözden Geçirme Tarihi	
Dokümanı Hazırlayan	**İç Kontrol**
Doküman Yayınını Onaylayan	**Yönetim Kurulu**

Değişiklik Takip Çizelgesi			
Sürüm No	**Değişiklik Tarihi**	**Değişikliği Yapan**	**Açıklama**
01	07.11.2024		2024 Yılı İlk Yayın

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. POLİTİKANIN AMACI VE DAYANAĞI

İşbu Kişisel Veri Saklama ve İmha Politikası (“Politika”), Allbatross Yatırım Menkul Değerler A.Ş. (‘’ Allbatross Yatırım’’ veya ‘’Şirket ‘’) tarafından Veri Sorumlusu sıfatıyla;

6698 Sayılı Kişisel Verileri Koruma Kanunu’nun 7’inci maddesinin 3’üncü fıkrası ile 22’nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği’ne uygun olarak; tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektedir.

Allbatross Yatırım; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanun’un 4. maddesinde sayılan genel ilkeler ile Kanun’un 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul Kararlarına ve işbu Politika’ ya uygun hareket etmektedir.

Veri saklama ve imha faaliyetlerine ek olarak kişisel verilerin işlenmesine ilişkin diğer hususlarda ayrıntılı bilgiye **Kişisel Verilerin İşlenmesi ve Korunması Politikası ’**ndan ulaşabilirsiniz.

2. POLİTİKANIN KAPSAMI

İşbu Politika Şirket tarafından verisi işlenen Yönetim Kurulu Üyeleri, çalışanları, çalışanların aile üyeleri ve yakınları, çalışan adayları, referans kişileri, tedarikçi çalışanları, tedarikçi yetkilileri, gerçek kişi tedarikçileri, müşterileri, potansiyel müşterileri, çağrı görüşmesi gerçekleştiren kişileri, ziyaretçileri ve diğer 3. kişilere ait işlenen kişisel verilerin;

- Kişisel veri işleme faaliyetlerinin yürütülmesi,
- Saklandığı kayıt ortamı,
- Saklanması ve imhasını gerektiren hukuki, teknik ya da diğer sebepler,
- İmha yöntemleri,
- Kişisel verilerin saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler,
- Saklama ve imha süreçlerinde yer alanların birimleri ve görev tanımları,
- Saklama ve imha sürelerini gösteren tablo,
- Periyodik imha sürelerini,
- İlgili kişinin talebi ile kişisel verilerinin silinmesi ve yok edilmesi ve süreleri,
- Şirketin veri sahibinin kişisel verilerinin silinmesine ilişkin talebini reddedebileceği durumları, kapsamaktadır.

3. KİŞİSEL VERİ İŞLEME FAALİYETLERİNİN YÜRÜTÜLMESİ

Allbatross Yatırım için kişisel verilerin güvenliğinin sağlanması bir çalışma prensibidir. Bu prensiple, kişisel veri işleme faaliyetleri Şirket adına düzenlenen politika ve prosedürlere uygun yürütülmektedir. Çalışanlar söz konusu Şirket politikalarına bağlı hareket edeceklerini Gizlilik Sözleşmesi ile taahhüt etmektedir.

Politikaların yürütülmesi, çalışan hareketlerinin politikalara uygunluğunun takibi, politikaların yayımlanması ve güncellenmesi, veri imha işlemlerinin gerçekleştirilmesi hususlarında sorumlu kişiler ve görev dağılımları belirlenmiştir.

Allbatross Yatırım, kişisel veri ileme faaliyetlerinin 6698 Sayılı Kişisel Verilerin Korunması Kanunu’na (‘’KVKK’’/’’Kanun’’) uygunluğu kapsamında gerekli denetimleri yapmakta/yaptırmaktadır. Sürecin yürütülmesinde alanında uzman kişilerden hizmet desteği alınabilmektedir.

Allbatross Yatırım tarafından gerekli denetimlerin yapılması/yaptırılmasında esnasında alınacak idari karar uygulamaya koyulacaktır.

Allbatross Yatırım çalışanları, kişisel veri ihlâline ilişkin herhangi bir bilgi alır, tespitte bulunur ya da bu konuda şüphe duymasını gerektirecek nitelikte bulgularla karşılaşırsa, bu durumu derhal ve 24(yirmi dört) saatten geç olmamak üzere en kısa sürede İç Denetim Sistemleri' ne bildirmekle yükümlüdür.

Tablo2: Saklama ve İmha Süreçlerinde Yer Alanların Birimleri ve Görev Tanımları

GÖREV TANIMLARI	DEPARTMAN/BİRİM
Veri sorumlusu ile ilgili kişi veya Kişisel Verileri Koruma Kurumu arasındaki iletişimin sağlanması	İrtibat Kişisi
Politikaların Yayımlanması ve Güncellenmesi	İç Denetim Sistemleri
Kişisel Veri İşleme Faaliyetlerine İlişkin Değişiklikleri Yetkili Birimlere/ Danışmana Bildirme	İç Denetim Sistemleri
Güvenlik Tedbirlerinin Değerlendirilmesi ve Güncellemelerin Bildirilmesi	Bilgi Teknolojileri
İnternet Sitesinde KVKK Aydınlatmalarının ve Politikalarının Yayımlanması ve Çerezler Hakkında Bilgilendirmelerin Gerçekleştirilmesi	Bilgi Teknolojileri
Çalışanlara Aydınlatma Yükümlülüğün Yerine Getirilmesini ve Eğitiminin Tamamlanmasını Sağlama	İnsan Kaynakları
Çalışan Hareketlerinin Politikaya Uygunluğunun Takibi/Denetimi	İnsan Kaynakları
Veri Silme, Yok Etme ve İmha İşlemlerinin Takibi	Bilgi Teknolojileri

4. KAYIT ORTAMLARI

Şirket tarafından, işbu Politikanın kapsamında sayılan gerçek kişilere ait kişisel veriler söz konusu verinin niteliğine ve işleme faaliyetine uygun olarak kayıt altına alınmaktadır.

Tablo 3: Elektronik ve Elektronik Olmayan Kayıt Ortamları

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
• Sistem Odası Sunucuları, • E-posta, • Departman Özelinde Ortak Klasörler, • Yazılımlar (Optimus, Aksis, Kobikom, SİEM), • Şirket bilgisayarları (Masaüstü, dizüstü), • Kamera Kayıt Cihazı, • Çağrı Merkezi Kayıt Cihazı,	• Arşiv, • Kilitli Dolap, • Sözleşmeler, • Kâğıt, • Klasörler, • Dosyalar, • Manüel veri kayıt sistemleri (bilgi toplama formları, izin formları, tutanak ve defterler gibi)

5. VERİ SAKLAMA

Allbatross Yatırım tarafından, işlenen kişisel veriler ilgili mevzuatta öngörülen süre boyunca veya böyle bir süre öngörülmemişse, kişisel verilerin işlenme amaçları için gerekli olan süre kadar saklanmaktadır.

Kişisel verilerin birden fazla amaç için işlendiği hallerde, verinin işlenme amaçlarının hepsinin ortadan kalkması durumunda re 'sen veya verilerin silinmesine mevzuatta bir engel olmaması ve ilgili kişinin talep etmesi durumunda veriler silinir, yok edilir veya anonim hale getirilir. İşlenen kişisel veriler aşağıda sayılan yürürlükte olan Kanun ve Yönetmelikler başta olmak üzere diğer ikincil düzenlemelerde öngörülen saklama süreleri kadar muhafaza edilmektedir.

Tablo 4: Veri Saklamayı Gerektiren Hukuki Sebepleri

VERİ SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER
6698 Sayılı Kişisel Verilerin Korunması Kanunu, 6098 Sayılı Türk Borçlar Kanunu, 213 Sayılı Vergi Usul Kanunu, 6102 Sayılı Türk Ticaret Kanunu, 6362 Sayılı Sermaye Piyasası Kanunu, Yatırım Hizmet ve Faaliyetleri ile Yan Hizmetlere İlişkin Belge ve Kayıt Düzeni Hakkında Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ-III-45.1.b ("Tebliğ III-45.1.b"), Aracı Kurumlar ve Portföy Yönetim Şirketleri Tarafından Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Tebliğ- III-42.1 ("Tebliğ III-42.1"), 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 4857 Sayılı İş Kanunu, 6361 Sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5.1. Saklamayı Gerektiren Sebepler

Elde edilen kişisel veriler; Allbatross Yatırım tarafından sunulan hizmetlerinin sürdürülebilmesi, yasal yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması amacıyla işbu Politikada düzenlenen kayıt ortamlarında, Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde aşağıdaki sebeplerle saklanmaktadır;

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

6. VERİ İMHA

Kişisel verileri imha etme (kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi) kişisel verilerin kullanıcıları tanımlayacak hiçbir bilgiye erişilemez ve tekrar kullanılamaz hale getirilmesidir.

6.1. İmhayı Gerektiren Sebepler

Kişisel veriler aşağıda sayılan durumlarda Şirket tarafından ilgili kişinin talebi üzerine ya da re 'sen silinir, yok edilir veya anonim hale getirilir:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya yürürlükten kaldırılması,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

7. KİŞİSEL VERİLERİ İMHA YÖNTEMLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler; Allbatross Yatırım tarafından re 'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

Allbatross Yatırım; kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin re 'sen karar alabilecek ve seçmiş olduğu kategoriye göre kullanacağı uygun yöntemi de serbestçe belirleyebilecektir.

7.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin silinmesi yöntemi olarak Şirket tarafından aşağıdaki yöntemlerden bir veya birkaçı kullanabilir:

Hizmet Olarak Kullanılan Bulut Çözümleri İçin	Silme komutu verilerek bulut tabanlı mail içeriğindeki kişisel veriler silinecektir. İşlemi yapan kişinin veri geri getirme yetkisi olmayacaktır.
Kâğıt Ortamında Bulunanlar İçin	Karartma yöntemi ile silinecektir. (İlgili kısım kesilerek) Mümkün değilse sabit mürekkep kullanılarak okunmayacak hale getirilecektir.
Merkezi Sunucudaki Ofis Dosyaları İçin	İşletim sisteminde (Windows) silme komutu ile silinecek veya dosya ve dosyaya ait dizindeki erişim hakları kaldırılacaktır. Silme ve kaldırma işlemini yapan kişi aynı zamanda sistem yöneticisi olmayacaktır.
Taşınabilir Medyaya Bulunan Veriler İçin	Şirket taşınabilir ortamlarda özel nitelikli kişisel veri bulundurmamaktadır. Kişisel verinin bu tip ortamda bulunması gerektiği durumlarda aşağıda belirtilen metotlarla silme işlemini uygulayacaktır: Kişisel veriler flash ortamında saklanması gerekirse şifreli olarak saklanacak ve bu yöntemlere uygun olarak silinecektir.

Veri Tabanları İçin	Kişisel Veri bulunan satır veri tabanı komutları (Delete vb.) ile silinecektir. İşlemi yapan kişi aynı zamanda veri tabanı yöneticisi olmayacaktır.

2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi yöntemi olarak Şirket tarafından aşağıdaki yöntemlerden bir veya birkaçını kullanabilir:

Yerel Sistemler İçin	De-manyetize Etme, Fiziksel Yok Etme (eritme, yok etme, toz haline getirme) Üzerine Yazma (optik medya üzerine en a 7 kez 0 ve 1'den oluşan rastgele veriler yazmak), bu yöntemlerden uygun olan bir ya da birkaçı seçilerek gerçekleştirilecektir.
Çevresel Sistemler İçin	Ağ cihazlarının çoğunda silme komutu vardır fakat yok etme özelliği bulunmamaktadır. Bu durumda yerel sistemlerde tercih edilen yöntemler uygulanabilir. Flash tabanlı sabit diskler destekleniyorsa ''blok erase'' desteklenmiyorsa yerel sistemlerde tercih edilen yöntemlerden biriyle yok edilebilir. Manyetik bantta saklanan veriler çok güçlü manyetik ortamlara maruz bırakılıp de-manyetize edilerek ya da fiziksel yöntemlerle yok edilir. (Yakma, eritme, küçük parçalara ayırma vb.) Sim kart ve hafıza alanlarında silme komutu yer almaktadır ancak yok etme komutu bulunmamaktadır. Bu sebeple yerel sistemlerden tercih edilen yöntem uygulanır. CD, DVD gibi optik diskler fiziksel yöntemlerle yok edilir. Veri kayıt ortamı çıkarılabilen yazıcılar, kayıt ortamı söküldükten sonra yerel sistemlerden uygun olan yöntemle yok edilir. Veri kayıt ortamı sabit olan yazıcılarda ise silme komutu yer almaktadır fakat yok etme seçeneği olmadığından yerel sistemler için tercih edilen yöntemlerden uygun olan seçilir.
Kâğıt ve Mikro Fiş Ortamları İçin	Kâğıt imha ve kırpma makinaları ile geri birleştirilemeyecek hale getirilecektir. Tarama yoluyla dijitale aktarım olursa yerel sistemlerdeki yok etme metotlarından biri ya da birkaçı kullanılacaktır.
Bulut Ortamı İçin	Hizmet alınan her bir bulut ortamı için kriptografik yöntemlerle şifreleme yapılacaktır. Hizmet sona erince anahtarlar kopyaları ile yok edilecektir. Cihazlar arıza ve bakıma gönderilmeden yok etme gerçekleştirilecek, gerçekleştirilemiyorsa veri depolama alanı sökülecektir. Bakım vb. için dışarıdan üçüncü kişi gelmesi durumunda ise olası kopyalama yapılmaması için tedbirler alınacaktır.

7.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır. Şirket kişisel verileri anonim hale getirmek için aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

Değer Düzensizliği Sağlamayan Yöntemler	
Değişkenleri Çıkarma	Değişkenlerden bir ya da birkaçı tablodan tamamen çıkartılır. Örneğin; Cinsiyet, doğum yeri, doğum tarihi, öğrenim durumu gibi bilgileri olduğu bir veri tabanında öğrenim durumu sütunu DELETE komutu ile silinmelidir.
Genelleştirme	Kişisel verilerin özelden genele çevrilmesidir. Raporlarda ve toplam değerlerin yer aldığı tablolarda kullanılmaktadır. Örneğin; inşaat ve yapı işi ile ilgilenen kişilerin genellikle doğal taş alması şeklindedir.

Değer Düzensizliği Sağlayan Yöntemler	
Gürültü Ekleme	Genelde sayısal değerler içeren veri kümelerine uygulanır. Seçilen değişken üzerine belirlenen ölçüde ekleme veya çıkarma yapılır. Oluşturulan bozulma her değere eşit ölçüde uygulanır. Örneğin; yaş, cinsiyet, il, gelir bilgilerinin yer aldığı bir tabloda değişken gelir olarak belirlenmişse her kayda +50,000 eklenerek yeni değerler satırlara yazılır.

ANONİM HALE GETİRMEYİ KUVVETLENDİRİCİ İSTATİSTİKİ YÖNTEMLER	
K-ANONİMLİK	Tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmaması için kullanılır. Örneğin; ad soyad, TC kimlik no, meslek olan bir veri kümesinde ad soyad ve TC kimlik no maskelenmiş halde girilmiş olsa da aynı değeri içeren tek kayıt varsa kişiyi tahmin etmek mümkün olur. Bu sebeple diğer değişkenlerden biri alınarak (x=1 yapılarak) tekrar sıralama yapılabilir.

8. SAKLAMA VE İMHA SÜRELERİ

Allbatross Yatırım, kişisel verileri işlendikleri amaç için gerekli yasal süreler boyunca saklar.

Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Mevzuatta öngörülmüş bir süre olmaması halinde kişisel veriler kişisel verilerin tutulması için azami süre boyunca saklanacaktır. Bu süreler verinin niteliği ve işleme amacına uygun olarak belirlenecektir.

Şirket'in ilgili kişisel veriyi kullanma amacı sona ermedi ise, ilgili mevzuat gereği söz konusu kişisel veri için öngörülen saklama süresi tabloda yer alan sürelerden fazla ise veya ilgili konuya ilişkin dava zamanaşımı süresi kişisel verinin tabloda yer alan sürelerden fazla saklanmasını gerektiriyorsa,

aşağıdaki tabloda yer alan süreler uygulanmayabilecektir. Bu halde kullanım amacı, özel mevzuat veya dava zamanaşımı süresinden hangisi daha sonra sona eriyor ise, o süre uygulama alanı bulacaktır.

Bu sürelerin sona ermesi dolayısıyla silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı durumda Şirket bu tarihi takip eden ilk periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir.

8.1. Periyodik İmha

Allbatross Yatırım, tarafından tespit edilen saklama ve imha süreleri, aşağıda ''Süreç Bazlı Veri Saklama ve İmha Sürelerine İlişkin Tablosu'' nda açıklanmıştır. Saklama süresi dolan kişisel veriler, işbu Politika 'da açıklanan imha süreleri çerçevesinde, 6 (altı) aylık periyodlarla işbu Politika 'da yer verilen usullere uygun olarak silinir, yok edilir veya anonim hale getirilir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanır.

Tablo 5: Süreç Bazlı Veri Saklama ve İmha Süreleri

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Yönetim Kurulu Üyelerine Ait Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşterilere Ait Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Tedarikçilere Ait Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Özlük Dosyalarına İlişkin Kişisel Veriler	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İş Sağlığı ve Güvenliği Mevzuatı Kapsamında İşlenen Kişisel Veriler	İş ilişkisinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Adaylarına Ait Kişisel Veriler	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Muhasebe ve Finansal İşlemlere İlişkin Tüm Kayıtlar	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çağrı Görüşmesi Kayıtları	10 yıl	Saklama süresi sonunda
Kamera Kayıtları	6 ay	Saklama süresi sonunda
Log Kayıları	2 yıl	Saklama süresi sonunda
Lokasyon Kayıtları	1 yıl	Saklama süresi sonunda
Silme Yok Etme Anonim Hale Getirme Kayıt Süreci	İşlem tarihinden itibaren 3 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

9. İLGİLİ KİŞİNİN TALEBİ İLE KİŞİSEL VERİLERİNİN SİLİNMESİ VE YOK EDİLMESİ VE SÜRELERİ

İlgili kişi, Kanunun 13'ncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir, her halde yapılan işleme binaen ilgili kişiye bilgi verir.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa; bu talep Şirket tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa; Şirket bu durumu üçüncü kişiye bildirir, üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

9.1. Şirketin Veri Sahibinin Kişisel Verilerinin Silinmesine İlişkin Talebini Reddedebileceği Durumlar:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarı faaliyetler kapsamında işlenmesi.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.
- Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.
- Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması.
- Orantısız çaba gerektiren taleplerde bulunulmuş olması.
- Talep edilen bilginin kamuya açık bir bilgi olması.

10. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER

Şirket Kanun'un 12. maddesine uygun olarak, kişisel verinin niteliğine göre gerekli idari ve teknik tedbiri almaktadır. Bu kapsamda gerekli denetimleri yapmakta/yaptırmakta olup kişisel verilerin kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesini, hukuka aykırı olarak açıklanması ve aktarılması engellenmektedir. Kişisel veri güvenliğine ilişkin gerekli teknik ve idari tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından kişisel verilerin ele geçirilmesi durumunda, Şirket mümkün olan en kısa süre içerisinde ilgili birimlere haber verecektir.

Tablo6: Şirket Tarafından Veri Güvenliğinin Sağlanması Amacıyla Alınan Tedbirler

VERİ GÜVENLİĞİ TEDBİRLERİ
• Ağ güvenliği ve uygulama güvenliği sağlanmaktadır. • Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır. • Anahtar yönetimi uygulanmaktadır. • Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır. • Çalışanlar için yetki matrisi oluşturulmuştur. • Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

11. YÜRÜRLÜLÜK

Bu Politika, Allbatross Yatırım Menkul Değerler A.Ş. Yönetim Kurulu' nun 07/11/2024 tarih ve 2024/67 sayılı kararı ile yürürlüğe girmiştir.

12. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Politikaya aykırı davranış tespit edildiğinde, aykırı davranan çalışan hakkında yapılacak değerlendirme sonrasında idari işlem uygulanabilecektir.

13. POLİTİKANIN GÜNCELLENMESİ

İşbu Politika, Kanun ve ilgili diğer mevzuat hükümlerinde meydana gelecek değişikliklerle uyumlu olarak güncellenebilecektir. Ayrıca, Allbatross Yatırım tarafından yürütülen kişisel veri saklama ve imha faaliyetlerinde de değişiklik olması durumunda gerekli güncellemeler yapılacaktır.

14. VERİ SORUMLUSUNA İLİŞKİN BİLGİLER

Unvanı : Allbatross Yatırım Menkul Değerler A.Ş.

Adresi : Huzur Mah. Azerbaycan Cad. Skyland Sitesi B No: 4B İç Kapı No:303 Sarıyer/İSTANBUL

Elektronik İletişim Adresi : kvkk@allbatrossyatirim.com

Kayıtlı Elektronik Posta Adresi : allbatrossyatirim@hs03.kep.tr

15. EKLER

Ek-1: Tanımları Düzenleyen Tablo

TANIMLAR	AÇIKLAMA
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan irade beyanıdır.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamdır.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.
Kişisel Verilerin Silinmesi	Kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu'dur.
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği
Kurul	Kişisel Verileri Koruma Kurulu'dur

Kurum	Kişisel Verileri Koruma Kurumu'dur.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişidir.
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
Veri ihlalleri	Kişisel verilerin kanuna aykırı şekilde ele geçirilmesi, toplanması, değiştirilmesi, kopyalanması, dağıtılması veya kullanılmasına dair haklı şüphelerin olduğu olaylardır.
İrtibat Kişisi	Veri sorumlusu ile ilgili kişi veya Kişisel Verileri Koruma Kurumu arasındaki iletişimin sağlanmasından sorumlu kişidir.

Ek-2: Kişisel Veri İmha Tutanağı