

JPMorgan Chase Bank, N.A., Columbus, Ohio- İstanbul Türkiye Şubesi & J.P. Morgan Menkul Değerler A.Ş. Gizlilik Politikası

Son Güncelleme: 28 Nisan 2022

1. Politika

Bu Politika, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**") ve ilgili ikincil mevzuatı ile ilgili diğer mevzuat (birlikte "**ilgili mevzuat**") uyarınca JPMorgan Chase Bank N.A. Columbus, Ohio - İstanbul Türkiye Şubesi ve J.P. Morgan Menkul Değerler A.Ş. tarafından her biri Veri Sorumlusu olarak ("**J.P. Morgan**", "**biz**" veya "**bizim**") müşteriler, kurumsal müşterilerin çalışanları ve tedarikçiler ile hizmetlerimizi alan diğer kişiler (birlikte, "**siz**") dahil olmak üzere etkileşime geçtiğimiz organizasyonumuz dışındaki kişiler için hazırlanmıştır. Bu Politika'da kullanılan tanımlı ifadeler Madde 11'de açıklanmıştır.

Bu Politika, Kişisel Verilerin İşlenmesine yönelik uygulamalarımızdaki değişiklikleri veya yürürlükteki kanunlarda yapılan değişiklikleri yansıtmak adına zaman zaman zaman değiştirilebilir veya güncellenebilir. Bu Politika'yı dikkatle incelemenizi ve bu Politika'nın hükümleri uyarınca yapabileceğimiz değişiklikleri gözden geçirmek için bu sayfayı düzenli olarak kontrol etmenizi öneriyoruz.

Aksi belirtilmedikçe, bu Politika'da yer alan bilgiler her iki J.P. Morgan kurumunun veri işleme faaliyetleri bakımından da geçerlidir.

2. Kişisel Verilerinizin İşlenmesi

Kişisel Verilerin Toplanması: Kişisel Verilerinizi aşağıda açıklandığı üzere çeşitli kaynaklardan topluyoruz:

- Kişisel Verilerinizi bizimle paylaştığınız hallerde topluyoruz (örn. e-posta veya telefon vasıtasıyla ya da başka yollarla bizimle iletişime geçtiğiniz haller).
- Kişisel Verilerinizi sizinle olan ilişkimizin olağan gidişatı sırasında topluyoruz (örn. işlemlerinizin yönetilmesi sırasında).
- Sosyal medya kullanımınız dâhil olmak üzere, alenileştirmeyi tercih ettiğiniz Kişisel Verileri topluyoruz (örn. profilinizi herkese görünür kıldığınız ölçüde, sosyal medya hesaplarınızdan bilgi toplayabiliriz).
- Üçüncü taraflardan size ait Kişisel Veriler alıyoruz (örn. işvereniniz, müşterilerimiz ve adli makamlar).
- Ürünlerimizi veya hizmetlerimizi üçüncü taraflar aracılığıyla satın aldığınız durumlarda, bu üçüncü taraflardan size ait kişisel veriler alıyoruz.

Kişisel Verilerin Üretilmesi: Yürürlükteki kanunlara tabi olmak kaydıyla, bizimle olan etkileşimlerine dair kayıtlar ve hesap bilgileriniz gibi sizinle ilgili Kişisel Veriler üretiyoruz.

İlgili Kişisel Veriler ve Hassas Kişisel Veriler: Yürürlükteki kanunlara tabi olmak kaydıyla, sizinle ilgili İşlediğimiz Kişisel Veri kategorileri aşağıdaki gibidir:

- *Kişisel bilgiler:* isim; mahlas; cinsiyet; doğum tarihi / yaş; medeni durumu; Sosyal Güvenlik numarası; pasaport numarası; devlet tarafından verilen diğer numaralar (vergi sicil numarası, sürücü belgesi numarası); uyruk; pasaport görüntüleri; sürücü belgeleri ve imzalar; fotoğraflar; görseller.
- *Aile bilgileri:* aile üyeleri ve bakılmakla yükümlü kimselerin isimleri ve iletişim bilgileri.
- *İletişim bilgileri:* adres; telefonu numarası; e-posta adresi ve sosyal medya hesap bilgileri.
- *İş bilgileri:* çalıştığı sektör; görevi; iş aktiviteleri; eski ve yeni işverenlerinin isimleri; iş adresi; iş telefon numarası; iş e-posta adresi;
- *Eğitim geçmişi:* eğitim ve yeterlilik bilgileri.
- *Finansal bilgiler:* fatura adresi; banka hesap numaraları; kredi kartı numaraları; kart sahibi veya hesap sahibi ismi ve bilgileri; talimat kayıtları; işlem bilgileri ve karşı taraf bilgileri.
- *İşitsel ve Görsel Kayıtlar:* Ticari faaliyetler kapsamında talep, talimat, alım ve işlemlere ilişkin telefon

görüşmeleri.

- *Fiziksel Mekân Güvenliği*: CCTV kayıtları.
- *Görüş ve fikirler*: Bize göndermeyi veya bizim hakkımızda yayınlamayı (sosyal medya platformlarında yayınlananlar dahil) tercih ettiğiniz her türlü görüş ve fikir.
- *Elektronik Tanımlama Verileri*: IP adresleri, çerezler, aktivite kayıtları, online belirleyiciler, eşsiz cihaz belirleyicileri ve konum belirleme verileri.

Hassas Kişisel Verilerinizin İşlenmesi: Aşağıdaki durumlar haricinde (uygulanabildiği hallerde) sizden Hassas Kişisel Veriler topluyor veya başka şekillerde Hassas Kişisel Verilerinizi işlemiyoruz:

- İşlemenin yürürlükteki kanunlarda öngörülmesi;
- Yürürlükteki kanunlara uygun olarak Hassas Kişisel Verilerinizin işlenmesine ilişkin önceden rızanızı aldığımız haller (yukarıda olduğu gibi, bu hukuki sebebe yalnızca İşlemenin gönüllük esaslı olarak yapıldığı hallerde dayanılır - İşlemenin kanunen zorunlu olduğu hallerde bu hukuki sebebe hiçbir şekilde dayanılmaz).

Kişisel Verilerinizi İşleme Amaçlarımız ve İşlemenin hukuki sebepleri: Yürürlükteki kanunlara tabi olmak kaydıyla, KVKK'nin 5. Maddesi ve 6. Maddesi uyarınca Kişisel Verilerinizi İşleme amaçlarımız ve Kişisel Verilerinizi İşlerken dayandığımız hukuki sebepler aşağıdaki gibidir:

İşleme amacı	İşlemenin hukuki sebebi
<i>Kara para aklamanın önlenmesi ve müşterinin belirlenmesi</i> : "Müşteriyi Tanıma" kontrolleri dâhil olmak üzere düzenleyici uyumluluk yükümlülüklerimizin yerine getirilmesi; kimliğinizin onaylanması ve doğrulanması (kredi referans kuruluşlarının kullanıldığı durumlar dahil); ve hükümetin, uluslararası örgütlerin (Avrupa Birliği ve Birleşmiş Milletler Güvenlik Konseyi dahil ancak bunlarla sınırlı olmamak üzere) ve/veya adli makamların yaptırım listeleri ile iç yaptırım listeleri ve diğer hukuki kısıtlamalara ilişkin denetim faaliyetlerinin yürütülmesi.	<ul style="list-style-type: none">• Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya;• İşlemenin bizimle yapabileceğiniz herhangi bir sözleşme ile bağlantılı olarak gerekli olması veya bizimle bir sözleşme akdetmek amacıyla yapacağınız işlemler için gerekli olması veya;• Kara para aklama, yaptırım ihlalleri ve dolandırıcılığın önlenmesi amaçlarıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde) veya;• İşlemeye ilişkin önceden rızanızı aldığımız durumlar (bu hukuki sebebe yalnızca İşlemenin gönüllük esaslı olarak yapıldığı hallerde dayanılır - İşlemenin gerekli veya zorunlu olduğu hallerde bu hukuki sebebe hiçbir şekilde dayanılmaz).
<i>Müşteri kabulü</i> : yeni müşterilerin kabulü ve iç uyum gerekliliklerine, politikalarına ve usullerine uyum sağlanması.	<ul style="list-style-type: none">• Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya;• İşlemenin bizimle yapabileceğiniz herhangi bir sözleşme ile bağlantılı olarak gerekli olması veya bizimle bir sözleşme akdetmek amacıyla yapacağınız işlemler için gerekli olması veya;• Yeni müşterilerin kabulü amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde) veya;• İşlemeye ilişkin önceden rızanızı aldığımız durumlar (bu hukuki sebebe yalnızca İşlemenin gönüllük esaslı olarak yapıldığı hallerde dayanılır - İşlemenin gerekli veya zorunlu olduğu hallerde bu hukuki sebebe hiçbir şekilde dayanılmaz).
<i>Size ürün ve hizmetlerin sunulması</i> : müşteri ilişkilerinin ve bankacılık ve/veya yatırım hizmetleri ile yan hizmetlerin yönetimi; talep edilen hizmetlerin sunulması için gerekli olan işlerin yapılması; bu hizmetlere ilişkin sizinle iletişime geçilmesi, ürün ve hizmetlerimizin geliştirilmesi ve iyileştirilmesi	<ul style="list-style-type: none">• Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya;• İşlemenin bizimle yapabileceğiniz herhangi bir sözleşme ile bağlantılı olarak gerekli olması veya bizimle bir sözleşme akdetmek amacıyla yapacağınız işlemler için gerekli olması veya;• Size ürün ve hizmet sunmak amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde) veya;• İşlemeye ilişkin önceden rızanızı aldığımız durumlar (bu hukuki sebebe yalnızca İşlemenin gönüllük esaslı olarak yapıldığı hallerde dayanılır - İşlemenin gerekli veya zorunlu olduğu hallerde bu hukuki sebebe hiçbir şekilde dayanılmaz).

<p><i>IT faaliyetleri:</i> iletişim sistemlerimizin yönetimi; IT güvenlik sistemlerinin işletilmesi ve IT güvenlik denetimlerinin yapılması</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • İşlemenin bizimle yapabileceğiniz herhangi bir sözleşme ile bağlantılı olarak gerekli olması veya bizimle bir sözleşme akdetmek amacıyla yapacağınız işlemler için gerekli olması veya; • IT sistemlerimizin yönetilmesi ve işletilmesi ile bu sistemlerin güvenliğinin sağlanması amacıyla İnternet Sitelerimizin faaliyetleri için İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde).
<p><i>Sağlık ve güvenlik:</i> sağlık ve güvenlik yönünden değerlendirmeler yapılması ve ilgili kayıtların tutulması ve ilgili hukuki yükümlülüklerin yerine getirilmesi.</p>	<p>Uygulanabildiği hallerde:</p> <ul style="list-style-type: none"> • İşlemenin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından gerçekleştirilmesi.
<p><i>Güvenlik:</i> tesislerimizin fiziksel güvenliğinin (tesise yapılan ziyaretlere ilişkin kayıtlar ve güvenlik kamerası kayıtları dahil) ve elektronik güvenliğinin (elektronik sistemlerimize eriştiğiniz durumlarda, giriş kayıtları ve erişim bilgileriniz dahil) sağlanması.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • İşletmemizin, tesislerimizin ve mal varlıklarımızın fiziksel ve elektronik güvenliğinin sağlanması amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde).
<p><i>Soruşturmalar:</i> yürürlükteki kanunlara uygun olarak, politikamızın ihlalinin ve suçların tespiti, soruşturma faaliyetlerinin yürütülmesi ve bu tür ihlal ve suçların önlenmesi.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • Politikalarımıza ve yürürlükteki kanunlara yönelik ihlallerin tespit edilmesi ve bu tür ihlallerin önlenmesi amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde).
<p><i>Kanunlara uyum:</i> resmi kurum ve kuruluşlarca öngörülen bilgi saklama, raporlama, bilgilendirme yükümlülüklerine uyulması dahil, yürürlükteki kanunlarda öngörülen hukuki ve düzenleyici yükümlülüklerimizin yerine getirilmesi.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması.
<p><i>Hukuki işlemler:</i> hakların tesis edilmesi, kullanılması ve korunması.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • Haklarımızın tesis edilmesi, kullanılması ve korunması amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde).

<p><i>Risk yönetimi:</i> Denetim, uyum, kontrol çalışmalarının ve risk yönetimine ilişkin diğer faaliyetler ile istihbarat, bilgi araştırmaları, kredibilite çalışmalarının yürütülmesi.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • İşletmemize yönelik risklerin yönetilmesi amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde).
<p><i>Dolandırıcılığın önlenmesi:</i> Dolandırıcılığın tespiti, önlenmesi ve soruşturulması.</p>	<ul style="list-style-type: none"> • Hukuki bir yükümlülüğün yerine getirilmesi için İşlemenin gerekli olması veya; • İşlemenin bizimle yapabileceğiniz herhangi bir sözleşme ile bağlantılı olarak gerekli olması veya bizimle bir sözleşme akdetmek amacıyla yapacağınız işlemler için gerekli olması veya; • Dolandırıcılığın tespit edilmesi ve önlenmesi amacıyla İşlemenin meşru menfaatlerimiz için gerekli olması (bu tür bir meşru menfaatin menfaatlerinize veya temel hak ve özgürlüklerinize zarar getirmediği ölçüde) veya; • İşlemeye ilişkin önceden rızanızı aldığımız durumlar (bu hukuki sebebe yalnızca İşlemenin gönüllük esaslı olarak yapıldığı hallerde dayanılır - İşlemenin gerekli veya zorunlu olduğu hallerde bu hukuki sebebe hiçbir şekilde dayanılmaz).

3. Kişisel Verilerin üçüncü kişilere açıklanması

Kişisel Verilerinizi, yürürlükteki kanunlara uygun olarak meşru ticari amaçlarımız uyarınca (size hizmet sunulması da dahil) J.P Morgan grubu bünyesindeki diğer şirketlere açıklayabiliriz. Kişisel Verilerinizi ayrıca aşağıdaki kişi ve kuruluşlara açıklayabiliriz:

- Yürürlükteki kanun veya düzenlemelere yönelik mevcut veya şüphelenilen ihlallerin bildirilmesi dahil olmak üzere, talep halinde veya gerektiği durumlarda, devlet daireleri, kanuni, düzenleyici veya benzeri makamlar, kamu denetçileri ve merkezi ve/veya yerel resmi kurumlar;
- bağlayıcı sözleşmesel gizlilik yükümlülüklerine tabi olmak kaydıyla, muhasebeciler, denetçiler, finansal danışmanları, avukatlar ve J.P Morgan'a dışarıdan hizmet veren diğer profesyonel danışmanlar;
- Madde 3'te belirtilen şartlara tabi olarak, dünyanın herhangi bir yerinde bulunan üçüncü taraf Veri İşleyenler (ödeme hizmet sağlayıcıları; nakliye şirketleri gibi)
- yürürlükteki kanunlar uyarınca hakların tesis edilmesi, kullanılması veya korunması için gerekli olduğu ölçüde, herhangi bir ilgili taraf, davacı, şikayetçi, soruşturmacı, adli makamlar veya mahkemeler;
- yürürlükteki kanunlar uyarınca kamu güvenliğine yönelik tehditlerin önlenmesi ve koruyucu önlemlerin alınması dahil olmak üzere, suçun önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ya da cezai yaptırımların uygulanması amacıyla herhangi bir ilgili tarafa;
- işletmemizin veya mali varlıklarımızın tamamını veya bir kısmını satmamız veya devretmemiz halinde (yeniden yapılanma, fesih veya tasfiye halleri dahil), herhangi bir üçüncü taraf alıcıya/alıcılara.

Kişisel Verilerinizin işlenmesi için bir üçüncü taraf Veri İşleyen ile çalışmamız halinde, Veri İşleyen, (i) Kişisel Verileri yalnızca önceden verilmiş yazılı talimatlarımıza uygun olarak İşlenmesine ve (ii) yürürlükteki kanunlarda öngörülen ek gereklilikler ile birlikte Kişisel Verilerin gizliliğini ve güvenliğini koruyucu önlemler alınmasına yönelik bağlayıcı sözleşmesel yükümlülüklerle tabi olacaktır.

4. Yurtdışına Kişisel Veri aktarımı

İşletmemizin uluslararası yapısı gereği, müşteri taleplerinin değerlendirilmesi, krediler, fon aktarımları ve diğer işlemlerin onay süreçleri veya yatırım ve aracılık hizmetleri gibi bazı ürünlerin ve hizmetlerin sunulması farklı J.P. Morgan kuruluşlarının sürece dahil olmasını zorunlu kılabilir. Örneğin, gerekli fonların sağlanabilmesi için farklı bir J.P. Morgan kuruluşunun hizmetlerine ihtiyaç duyabiliriz ve bu hizmetlerin sağlanabilmesi için ilgili kuruluşlarla Kişisel Veri paylaşmamız gerekebilir. Benzer şekilde, kurumsal yapımız gereği belirli işlemlerin gerçekleştirilebilmesi için onaya veya farklı bir J.P. Morgan kuruluşunda çalışan bir görevlinin onayına ihtiyaç duyabiliriz.

Bu gibi durumlarla sınırlı olmak üzere ve zorunlu olduğu hallerde, işbu Politika'da öngörülen amaçlarla bağlantılı olarak Kişisel Verilerinizi J.P. Morgan grubu bünyesindeki diğer şirketlere veya Madde 3'te yer alan üçüncü taraflara aktarmamız gerekebilir. Bu sebeple, Kişisel Verilerinizi, ilgili mevzuat kapsamında daha düşük standartlar öngören veri koruma kanunları da dahil olmak üzere farklı kanun ve veri koruma uyum gerekliliklerinin bulunduğu diğer ülkelere aktarabiliriz.

Kişisel Verilerinizi aşağıdakileri esas alarak diğer ülkelere aktarıyoruz:

- Veri Koruma Kurumunun yeterli veri koruması kriterinin sağlandığına ilişkin tespit kararları ve veri aktarımına yönelik tedbirleri;
- Bağlayıcı Kurumsal Kurallarımız;
- uygun Standart Sözleşme Maddeleri;
- açık rızanız gibi diğer geçerli veri aktarımı mekanizmaları.

Yurtdışına veri aktarımları için uygulanan tedbirlere yönelik daha fazla bilgi almak için Madde 10'da yer alan iletişim bilgilerinizi kullanarak bize ulaşabilirsiniz.

5. Veri Güvenliği

Kişisel Verilerinizin kazaen veya hukuka aykırı olarak yok edilmesine, kaybına, değiştirilmesine, yetkisiz olarak ifşa edilmesine, erişilmesine ve başka şekilde hukuka aykırı veya yetkisiz olarak İşlenmesine karşı korunması için yürürlükteki kanunlara uygun teknik ve idari güvenlik tedbirleri alıyoruz.

Bize gönderdiğiniz Kişisel Verilerin, güvenli bir şekilde gönderilmesini temin etmek ise sizin sorumluluğunuz altındadır.

6. Verilerin Doğruluğu

Aşağıdakileri temin etmek için gerekli adımları atıyoruz:

- İşlediğimiz Kişisel Verilerinizin doğru ve gerektiği durumlarda, güncel tutulması ve
- İşlediğimiz Kişisel Verilerinizin yanlış olması halinde (bu verilerin İşlenme amaçları dikkate alınarak) silinmesi veya gecikmeksizin düzeltilmesi.

Zaman zaman Kişisel Verilerinizin doğruluğunu teyit etmenizi isteyebiliriz.

7. Veri Minimizasyonu

İşlediğimiz Kişisel Verilerin, işbu Politika'da öngörülen amaçlarla bağlantılı olarak makul ölçüde gereken Kişisel Veriler ile sınırlı olmasını sağlamak için gerekli adımları atıyoruz.

8. Verilerin Saklanması

Kişisel Verilerinizin yalnızca bu Politika'da belirlenen amaçlar için gerekli olan en kısa süre boyunca İşlenmesini sağlamak için gerekli adımları atıyoruz. Kişisel Verilerinize yönelik saklama sürelerinin belirlenmesi için kullandığımız kriterler aşağıdaki gibidir:

(1) Kişisel Verilerinizin kopyalarını, tanımlanmanıza izin verecek bir şekilde yalnızca aşağıdaki hallerde saklayacağız:

- a. Sizinle devam eden bir ilişkimizin olması halinde (örn. hizmet alıcısı olmanız veya yasal olarak e-posta listemizde yer aldığınız ve aboneliğinizi iptal etmediğiniz hallerde); veya
- b. Geçerli bir hukuki sebebimizin bulunduğu durumlarda, Kişisel Verilerinizin saklanması bu Politika'da öngörülen kanuni amaçlarla bağlantılı olarak gerekli olması (örn. Kişisel Verilerinizin işvereniniz ile aramızdaki bir sözleşmeye dahil olduğu ve söz konusu sözleşmedeki yükümlülüklerimizin yerine getirilmesi ve işletmemizin operasyonu amaçlarıyla bu verileri işlemenin **meşru** menfaatlerimiz için gerekli olması veya Kişisel Verilerinizin saklanmasına yönelik kanuni bir yükümlülüğümüzün bulunduğu haller),

ve:

(2) ařağıdaki süreler boyunca saklayacağız:

- a. yürürlükteki kanunlar kapsamında ilgili zamanaşımı süresi (diđer bir deyişle, saklama süreleri veya herhangi bir kişinin bize karşı Kişisel Verileriniz ile bağlantılı veya Kişisel Verilerinizi ilgilendirebilecek bir hukuki talepte bulunabileceđi süre); ve
- b. söz konusu ilgili zamanaşımı süresinin sona ermesinden itibaren bir (1) yıllık ek süre (böylece, herhangi bir kişinin zamanaşımı süresinin sonunda bir hukuki talepte bulunması halinde, bu talebi ilgilendiren Kişisel Verilerin tespiti için makul bir süreimiz olacaktır)

ve:

(3) ayrıca, ilgili hukuki talebin ileri sürülmesi halinde, Kişisel Verilerinizi bu taleple bağlantılı olarak gereken ek süreler boyunca İşleyebiliriz.

Paragraf (2)a ve (2)b'de belirtilen süreler boyunca, Kişisel Verilerin herhangi bir hukuki talep ile veya yürürlükteki kanunlar kapsamındaki herhangi bir yükümlülükle bağlantılı olarak incelenmesi gereken haller hariç olmak üzere, Kişisel Verilerinizin İşlenmesini, bu verilerin depolanması ve güvenliğinin sağlanması ile sınırlandıracağız.

Paragraf (1), (2) ve (3)'te yer alan sürelerin, her biri için uygulanabildiđi ölçüde, sona ermesi halinde:

- ilgili Kişisel Verileri kalıcı olarak sileceğiz veya yok edeceğiz;
- Kişisel Verilerinizi kullanılmayacak şekilde arşivleyeceğiz veya
- ilgili Kişisel Verileri anonimleştireceğiz.

Saklama sürelerine ilişkin sorularınız için ařağıda yer verilen bilgiler üzerinden bizimle irtibata geçebilirsiniz.

9. Haklarınız

KVKK'nin 11. Maddesi uyarınca Kişisel Verilerinizle ilgili olarak ařağıdaki haklara sahipsiniz:

- Kişisel Verilerinizin işlenip işlenmediđini öğrenme;
- Eğer işlenmişse buna ilişkin bilgi talep etme;
- Kişisel Verilerinizin işlenme amacını ve Kişisel Verilerinizin bu amaçlara uygun kullanılıp kullanılmadığını öğrenme;
- Yurt içinde ve yurt dışında Kişisel Verilerinizin aktarıldığı üçüncü kişileri bilme;
- Kişisel Verilerinizin eksik veya yanlış işlenmesi halinde bunların düzeltilmesini isteme;
- KVKK'nin 7. Maddesinde öngörülen şartlar çerçevesinde Kişisel Verilerinizin silinmesini veya yok edilmesini isteme;
- Yukarıdaki iki madde uyarınca yapılan işlemlerin, Kişisel Verilerinizin aktarıldığı üçüncü kişilere bildirilmesini isteme;
- İşlenen Kişisel Verilerinizin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhinize bir sonucun ortaya çıkmasına itiraz etme;
- Kişisel Verilerinizin kanuna aykırı olarak işlenmesi sebebiyle zarara uğramanız hâlinde zararın giderilmesini talep etme.

Bu haklardan bir veya daha fazlasını kullanmak veya haklarınız, işbu Politika'nın diđer herhangi bir hükmü ya da Kişisel Verilerinizi İşlememiz hakkında herhangi bir soru sormak için, Madde 10'da verilen iletişim bilgilerinizi kullanarak bizimle iletişime geçebilirsiniz.

Başvurunuzda konu talepler içeriđe bađlı olarak en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırılacaktır. Bununla birlikte, taleplerinizin karşılanmasının bizim için ek bir masraf doğurması halinde Veri Koruma Kurumu tarafından belirlenen tarifedeki ücretler tarafınızdan talep edilebilecektir.

10. İletişim Bilgileri

İşbu Politika'da yer alan bilgiler veya Kişisel Verilerinizin J.P. Morgan tarafından İşlenmesiyle ilgili herhangi bir konu hakkında herhangi bir yorumunuz, sorunuz veya endişeniz olması halinde, lütfen J.P. Morgan müşteri hizmetleri temsilciniz ile veya ařağıdaki adres üzerinden bizimle irtibata geçin:

JPMorgan Chase Bank, N.A., Columbus, Ohio-İstanbul Türkiye Şubesi
Büyükdere Cad. Kanyon Ofis Binası No:185, 34394 Bevent Beşiktaş, İstanbul, Türkiye

11. Tanımlar

Çalışanlar	Mevcut, eski ve aday yöneticiler, yetkililer, danışmanlar, çalışanlar, geçici personel, bireysel yükleniciler, stajyerler, geçici görevlendirmeyle çalışanlar ve diğer personel.
Hassas Kişisel Veri	Kişilerin ırk veya etnik kökeni, siyasi düşüncesi, dini veya felsefi inançları, kılık kıyafeti, dernek, vakıf veya sendika üyeliği, bedensel ve ruhsal sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri veya yürürlükteki kanunlar uyarınca hassas kişisel veri kabul edilebilecek diğer bilgiler.
İşlemek, İşlenen veya İşleme	Toplama, kaydetme, organize etme, yapılandırma, depolama, değiştirme veya uyarılama, kurtarma, konsültasyon, kullanma, aktarma yoluyla açıklama, yayma veya başka şekilde erişilebilir hale getirme, gruplama veya birleştirme, sınırlama, silme veya yok etme gibi, otomatik olan veya olmayan yollarla, Kişisel Veriler ile ilgili yapılan tüm işlemler.
Kişisel Veri	Herhangi bir kişi hakkındaki veya herhangi bir kişiyi belirlenebilir kılan bilgi.
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Veri İşleyen	Veri Sorumlusu adına Kişisel Veri işleyen herhangi bir gerçek veya tüzel kişi (Veri Sorumlusunun çalışanları dışındaki).
Veri Koruma Kurumu	Türkiye Kişisel Verileri Koruma Kurumu İnternet Sitesi: https://kvkk.gov.tr/ Telefon: 198 / 0312 216 50 00
Veri Sorumlusu	Kişisel Verilerin işleme amaçlarını ve vasıtalarını belirleyen kişi. Pek çok ülkede Veri Sorumlusu, yürürlükteki veri koruma kanunlarına uyulmasından birinci derecede sorumludur.

JPMorgan Chase Bank, N.A., Columbus, Ohio-Istanbul Turkey Branch & J.P. Morgan Menkul Değerler A.Ş. Privacy Policy

Last Update: April 28, 2022

1. This Policy

This Policy is issued by JPMorgan Chase Bank, N.A., Columbus, Ohio-Istanbul Turkey Branch and J.P. Morgan Menkul Değerler A.Ş. on behalf of themselves, each as the Controller (hereinafter referred to as “**J.P. Morgan**”, “**we**”, “**us**” or “**our**”) in accordance with the Law No. 6698 on Protection of Personal Data (“**Data Protection Law**”) and its secondary legislation along with any other applicable laws,(together, “**applicable law**”); and is addressed to individuals outside our organisation with whom we interact, customers, Personnel of corporate customers and vendors, and other recipients of our services (together, “**you**”). Defined terms used in this Policy are explained in Section 11 below.

This Policy may be amended or updated from time to time to reflect changes in our practices with respect to the Processing of Personal Data, or changes in applicable law. We encourage you to read this Policy carefully, and to regularly check this page to review any changes we might make in accordance with the terms of this Policy.

Unless stated otherwise, the information within this Policy applies to the processing activities of both J.P. Morgan entities.

2. Processing your Personal Data

Collection of Personal Data: We collect Personal Data about you from a variety of sources as follows:

- We obtain your Personal Data when you provide it to us (e.g., where you contact us via email or telephone, or by any other means).
- We collect your Personal Data in the ordinary course of our relationship with you (e.g., in the course of managing your transactions).
- We collect Personal Data that you manifestly choose to make public, including via social media (e.g., we may collect information from your social media profile(s), to the extent that you choose to make your profile publicly visible).
- We receive your Personal Data from third parties who provide it to us (e.g., your employer; our customers; and law enforcement authorities).
- We receive your personal data from third parties, where you purchase any of our products or services through such third parties.

Creation of Personal Data: We create Personal Data about you, such as records of your interactions with us, and details of your accounts, subject to applicable law.

Relevant Personal and Sensitive Personal Data: The categories of Personal Data about you that we Process, subject to applicable law, are as follows:

- *Personal details:* given name(s); preferred name(s); gender; date of birth / age; marital status; Social Security number; passport number(s); other government issued number(s) (tax identification number(s), driving license number(s)); nationality; images of passports, driving licenses, and signatures; photographs; visual images.
- *Family details:* names and contact details of family members and dependents.
- *Contact details:* address; telephone number; email address; and social media profile details.
- *Employment details:* industry; role; business activities; names of current and former employers; work address; work telephone number; work email address.
- *Education history:* details of your education and qualifications.
- *Financial details:* billing address; bank account numbers; credit card numbers; cardholder or

accountholder name and details; instruction records; transaction details; and counterparty details.

- *Audio and Visual Records:* Phone conversations regarding requests, orders, purchases and transactions within the scope of commercial activities.
- *Physical Property Security:* CCTV records.
- *Views and opinions:* any views and opinions that you choose to send to us, or publish about us (including on social media *platforms*).
- *Electronic Identifying Data:* IP addresses; cookies; activity logs; online identifiers; unique device identifiers; and geolocation data.

Processing your Sensitive Personal Data: We do not seek to collect or otherwise Process your Sensitive Personal Data, except where (as applicable):

- the Processing is stipulated under the applicable law;
- we have, in accordance with applicable law, obtained your explicit consent prior to Processing your Sensitive Personal Data (as above, this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is obligatory in any way); or

Purposes for which we may Process your Personal Data, and legal bases for Processing: The purposes for which we may Process Personal Data, subject to applicable law, and the legal bases on which we may perform such Processing per Article 5 and Article 6 of the Data Protection Law, are:

Processing purpose	Legal basis for Processing
<p><i>AML/KYC:</i> fulfilling our regulatory compliance obligations, including ‘Know Your Client’ checks; and confirming and verifying your identity (including by using credit reference agencies); and screening against government, supranational bodies (including but not limited to the European Union and the United Nations Security Council) and/or law enforcement agency sanctions lists as well as internal sanctions lists and other legal restrictions.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • The Processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the Processing for the purposes of preventing money laundering, sanctions violations and protecting against fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
<p><i>Client on-boarding:</i> on-boarding new clients; and compliance with our internal compliance requirements, policies and procedures.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • The Processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the Processing for the purpose of on-boarding new clients (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms). • We have obtained your prior consent to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
<p><i>Provision of products and services to you: administering relationships and banking and/or investment related services as well as their ancillary services; performance of tasks necessary for the provision of the requested services; communicating with you in relation to those services, improve our products and services.</i></p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • The Processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the Processing for the purpose of providing products and services to you (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

<p><i>IT operations:</i> management of our communications systems; operation of IT security; and IT security audits.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • The Processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the Processing for the purpose of managing and operating our IT systems and ensuring the security of those systems (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p><i>Health and safety:</i> health and safety assessments and record keeping; and compliance with related legal obligations.</p>	<p>As applicable:</p> <ul style="list-style-type: none"> • The Processing is conducted by individuals or authorized entities and institutions who are under confidentiality obligations for protection of public health, protective health services, medicinal diagnosis, treatment and care services; and planning and management of health services and its financing; or • We have obtained your prior consent to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is obligatory in any way).
<p><i>Security:</i> physical security of our premises (including records of visits to our premises and CCTV recordings); and electronic security (including login records and access details, where you access our electronic systems).</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the Processing for the purpose of ensuring the physical and electronic security of our business, premises, and assets (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p><i>Investigations:</i> detecting, investigating and preventing breaches of policy, and criminal offences, in accordance with applicable law.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the Processing for the purpose of detecting, and protecting against, breaches of our policies and applicable laws (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p><i>Legal compliance:</i> compliance with our legal and regulatory obligations under applicable law, including information, reporting, notification obligations regulated by public institutions and authorities.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation.
<p><i>Legal proceedings:</i> establishing, exercising and defending legal rights.</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the Processing for the purpose of establishing, exercising or defending our legal rights (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p><i>Risk Management:</i> Audit, compliance, controls and other risk management as well as intelligence, data research and credibility assessments</p>	<ul style="list-style-type: none"> • The Processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the Processing for the purpose of managing risks to which our business is exposed (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).

Fraud prevention: Detecting, preventing and investigating fraud.

- The Processing is necessary for **compliance with a legal obligation**; or
- The Processing is **necessary in connection with any contract** that you may enter into with us, or to take steps prior to entering into a contract with us; or
- We have **a legitimate interest** in carrying out the Processing for the purpose of detecting, and protecting against, fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
- We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

3. Disclosure of Personal Data to third parties

We may disclose your Personal Data to other entities within the J.P. Morgan group, for legitimate business purposes (including providing services to you), in accordance with applicable law. In addition, we may disclose your Personal Data to:

- Governmental, legal, regulatory, or similar authorities, ombudsmen, and central and/or local government agencies, upon request or where required, including for the purposes of reporting any actual or suspected breach of applicable law or regulation;
- accountants, auditors, financial advisors, lawyers and other outside professional advisors to J.P. Morgan, subject to binding contractual obligations of confidentiality;
- third party Processors (such as payment services providers; shipping companies; etc.), located anywhere in the world, subject to the requirements noted below in this Section [3](#);
- any relevant party, claimant, complainant, enquirer, law enforcement agency or court, to the extent necessary for the establishment, exercise or defense of legal rights in accordance with applicable law;
- any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security in accordance with applicable law;
- any relevant third party acquirer(s), in the event that we sell or transfer all or any relevant portion of our business or assets (including in the event of a reorganization, dissolution or liquidation);

If we engage a third-party Processor to Process your Personal Data, the Processor will be subject to binding contractual obligations to: (i) only Process the Personal Data in accordance with our prior written instructions; and (ii) use measures to protect the confidentiality and security of the Personal Data; together with any additional requirements under applicable law.

4. International transfer of Personal Data

Because of the international nature of our business, certain products and services may require the involvement of other J.P. Morgan entities such as evaluation of customer requests, necessary approvals for loans or investment services, intermediary services, transfer of funds, and other transactions. For example, we may need to employ the services of another J.P. Morgan entity to secure necessary funds and it might be necessary to share Personal Data with them for provision of such services. Similarly, we may need approval or approval from an officer at another J.P. Morgan entity for certain transactions due to our organizational structure.

In such cases and provided that it is necessary, we may need to transfer your Personal Data within the J.P. Morgan group, and to third parties as noted in Section [3](#) above, in connection with the purposes set out in this Policy. For this reason, we may transfer your Personal Data to other countries that may have different laws and data protection compliance requirements, including data protection laws of a lower standard to those that apply under applicable law.

Where we transfer your Personal Data to other countries, we do so on the basis of:

- adequacy decisions and data transfer measures by the Data Protection Authority;
- our Binding Corporate Rules;
- suitable Standard Contractual Clauses;
- other valid transfer mechanisms such as your prior consent .

If you want to receive more information about the safeguards applied to international transfers of personal data, please use the contact details provided in Section 10 below.

5. Data Security

We have implemented appropriate technical and organizational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of Processing, in accordance with applicable law.

You are responsible for ensuring that any Personal Data that you send to us are sent securely.

6. Data Accuracy

We take reasonable steps designed to ensure that:

- your Personal Data that we Process are accurate and, where necessary, kept up to date; and
- any of your Personal Data that we Process that are inaccurate (having regard to the purposes for which they are Processed) are erased or rectified without delay.

From time to time we may ask you to confirm the accuracy of your Personal Data.

7. Data Minimisation

We take reasonable steps designed to ensure that your Personal Data that we Process are limited to the Personal Data reasonably required in connection with the purposes set out in this Policy.

8. Data Retention

We take reasonable steps designed to ensure that your Personal Data are only Processed for the minimum period necessary for the purposes set out in this Policy. The criteria for determining the duration for which we will retain your Personal Data are as follows:

- (1) we will retain copies of your Personal Data in a form that permits identification only for as long as:
 - a. we maintain an ongoing relationship with you (e.g., where you are a recipient of our services, or you are lawfully included in our mailing list and have not unsubscribed); or
 - b. your Personal Data are necessary in connection with the lawful purposes set out in this Policy, for which we have a valid legal basis (e.g., where your Personal Data are included in a contract between us and your employer, and we have **a legitimate interest** in processing those data for the purposes of operating our business and fulfilling our obligations under that contract; or where we have a legal obligation to retain your Personal Data),

plus:

- (2) the duration of:
 - a. any applicable limitation period under applicable law (i.e., retention periods and any period during which any person could bring a legal claim against us in connection with your Personal Data, or to which your Personal Data may be relevant); and
 - b. an additional one (1) year period following the end of such applicable limitation period (so that, if a person bring a claim at the end of the limitation period, we are still afforded a reasonable amount of time in which to identify any Personal Data that are relevant to that claim),

and:

- (3) in addition, if any relevant legal claims are brought, we may continue to Process your Personal Data for such additional periods as are necessary in connection with that claim.

During the periods noted in paragraphs (2)a and (2)b above, we will restrict our Processing of your Personal Data to storage of, and maintaining the security of, those data, except to the extent that those data need to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once the periods in paragraphs (1), (2) and (3) above, each to the extent applicable, have concluded, we will either:

- permanently delete or destroy the relevant Personal Data;
- archive your Personal Data so that it is beyond use; or

- anonymize the relevant Personal Data.

Please contact us using the details below should you have any questions on the applicable retention periods.

9. Your legal rights

According to Article 11 of the Data Protection Law, you are entitled to certain rights with respect to your Personal Data including:

- to learn whether your Personal Data is processed;
- if it is processed, to request information with regard to such processing;
- to learn the purposes of the processing and whether your Personal Data is used for such purpose or not;
- to know the third persons within or outside the country to whom your Personal Data is transferred;
- to request correction of your Personal Data if the data is processed incompletely or inaccurately;
- to request deletion or destruction of your Personal Data under the conditions set forth in Article 7 of the Data Protection Law;
- to request notification of third parties, to whom your Personal Data is transferred, concerning the actions taken within the scope of the foregoing two items;
- to object to the consequences to detriment of yourself, as a result of the analysis of your Personal Data exclusively by automatic means;
- to claim indemnification if you suffered damages due to illegal processing of your Personal Data;

To exercise one or more of these rights, or to ask a question about these rights or any other provision of this Policy, or about our Processing of your Personal Data, please use the contact details provided in Section 10 below.

The requests found in your application will be resolved as soon as possible according to the nature of your request and within thirty days at the latest free of charge. However, if your request incurs additional cost to us, then you may be charged over the tariff fee determined by the Data Protection Authority.

10. Contact details

If you have any comments, questions or concerns about any of the information in this Policy, or any other issues relating to the Processing of Personal Data by J.P. Morgan, please contact your regular J.P. Morgan client service contact, or:

JPMorgan Chase Bank, N.A., Columbus, Ohio-İstanbul Turkey Branch,
Büyükdere Cad. Kanyon Ofis Binası No:185, 34394 Levent Beşiktaş, İstanbul, Turkey

J.P. Morgan Menkul Değerler A.Ş.
Büyükdere Cad. Kanyon Ofis Binası No:185, 34394 Levent Beşiktaş, İstanbul, Turkey

11. Defined terms

Controller	The entity that decides how and why Personal Data is Processed. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.
Data Protection Authority	Personal Data Protection Authority of Turkey Website: https://kvkk.gov.tr/ Phone: 198 / 0312 216 50 00

Data Protection Law	The Law No. 6698 on Protection of Personal Data
Personal Data	Information that is about any individual, or from which any individual is identifiable.
Process or Processed or Processing	Anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personnel	Any current, former and prospective directors, officers, consultants, employees, temporary staff, individual contractors, interns, secondees and other personnel.
Processor	Any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).
Sensitive Personal Data	Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, clothing and attire, trade union, association or union membership, physical or mental health, sexual life, criminal convictions and security measures; and biometric and genetic data or any other information that may be deemed to be sensitive under applicable law.