



Yasal Süreç Yönergeleri

ABD Dışındaki Devlet Kurumları ve Emniyet Teşkilatları

Bu yönergeler, ABD dışındaki devlet kurumları ve emniyet teşkilatlarının ilgili bölgedeki veya ülkedeki Apple kuruluşlarından Apple aygıtlarının, ürünlerinin ve hizmetlerinin müşterileri hakkında bilgi istemesi durumunda kullanılmak üzere sunulmaktadır. Apple, bu Yönergeleri gerektiği şekilde güncelleyecektir.

Apple, bu Yönergelerde belirli bir bölge veya ülkedeki müşteri bilgilerinden sorumlu ilgili tüzel kişi anlamına gelir. Küresel bir şirket olarak Apple, farklı yetki bölgelerinde topladığı ve Apple Inc. tarafından kendi adına işlenen kişisel bilgilerden sorumlu çok sayıda tüzel kişiliğe sahiptir. Örneğin, ABD dışındaki Apple perakende kuruluşlarında bulunan satış noktası bilgileri Apple'ın her ülkedeki ayrı perakende kuruluşları tarafından denetlenmektedir. Apple.com ve Apple Medya Hizmetleri ile ilgili kişisel bilgiler, belirli bir yargı bölgesi dahilindeki her hizmetin koşullarında yansıtıldığı şekilde ABD dışındaki tüzel kişiler tarafından da kontrol edilebilir. Genel anlamda, Apple'ın ABD dışında Avustralya, Kanada, İrlanda ve Japonya'daki tüzel kişilikleri, kendi bölgelerindeki Apple hizmetleriyle ilgili müşteri verilerinden sorumludur.

Bilgilerin ifşa edilmesi hakkındaki müşteri soruları da dahil olmak üzere, Apple müşterileri ile ilgili diğer tüm bilgi talepleri www.apple.com/tr/privacy/contact/ adresine yönlendirilmelidir. Bu Yönergeler, ABD'deki devlet kurumları ve emniyet teşkilatları tarafından Apple Inc.'e iletilen talepler için geçerli değildir.

Apple olarak, devlet kurumları ve emniyet teşkilatları tarafından iletilen bilgi talepleri için, verilerimizi kontrol eden küresel kuruluşlarla ilgili yasalara uyar ve bilgileri yasal olarak gerekli olduğu şekilde sağlarız. Acil durumlar (aşağıda Acil Talepler bölümünde tanımlanmıştır) dışında, ABD dışındaki devlet kurumları ve emniyet teşkilatlarından gelen tüm içerik talepleri, ABD Elektronik Haberleşmenin Gizliliği Kanunu (ECPA) dahil olmak üzere geçerli yasalara uygun olmalıdır. Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Yasası ("CLOUD Yasası Anlaşması") uyarınca, Karşılıklı Adli Yardımlaşma Anlaşması veya bir Yürütme Anlaşması kapsamındaki talepler ECPA ile uyumludur. Apple, müşteriyle ilgili içeriği, müşterinin hesabında bulunduğu haliyle, yalnızca yasal olarak geçerli bir sürece cevaben sağlar.

Apple, özel sektör temsilcilerinden gelen talepler için, müşteri verilerini kontrol eden yerel kuruluşlarla ilgili yasalara uyar ve yasal olarak gerekli verileri sağlar.

Apple; devlet kurumları, emniyet teşkilatları ve özel sektör temsilcilerinden gelen meşru yasal talepleri almaya, takip etmeye, işlemeye ve bunlara yanıt vermeye yönelik merkezi bir sürece sahiptir. Bu süreç, taleplerin alındığı andan itibaren bunlara yanıt verilene kadar geçerlidir. Hukuk departmanımızda çalışan eğitimli bir ekip, alınan tüm talepleri inceler ve değerlendirir. Apple'ın, geçerli bir yasal dayanağı olmadığını belirlediği veya belirsiz, uygunsuz ya da aşırı kapsamlı olduğunu düşündüğü taleplere itiraz edilir, karşı çıkılır veya bu talepler reddedilir.

Apple, yanıtları, talepte bulunan yetkilinin emniyet teşkilatındaki resmi e-posta adresi üzerinden talepte bulunan emniyet teşkilatına iletir. Apple tarafından sağlanan yanıtlar çerçevesinde tüm kanıtların

korunması, talepte bulunan emniyet teşkilatının sorumluluğundadır.

DİZİN

I. Genel Bilgiler

II. Apple'a Gönderilen Yasal Talepler

- A. Devlet Kurumları ve Emniyet Teşkilatlarının Bilgi Talepleri
- B. Devlet Kurumları ve Emniyet Teşkilatlarının Bilgi Taleplerini Yönetme ve Cevaplama
- C. Koruma Talepleri
- D. Acil Talepler
- E. Hesap Kısıtlama/Silme Talepleri
- F. Müşterinin Bilgilendirilmesi

III. Apple'dan Alınabilecek Bilgiler

- A. Aygıt Kaydı
- B. Müşteri Hizmetleri Kayıtları
- C. Apple Medya Hizmetleri
- D. Apple Store İşlemleri
- E. Apple.com Siparişleri
- F. Hediye Kartları
- G. Apple Pay
- H. iCloud
- I. Bul
- J. AirTag ve Bul Ağı Aksesuar Programı
- K. Parola ile Kilitlenmiş iOS Aygıtlarından Verilerin Çıkarılması
- L. IP Adresi Talebi
- M. Alınabilecek Diğer Aygıt Bilgileri
- N. Apple Store CCTV Verilerine Yönelik Talepler
- O. Game Center
- P. iOS Aygıt Aktivasyonu
- Q. Bağlantı Günlükleri
- R. Apple ID'm ve iForgot Günlükleri
- S. FaceTime
- T. iMessage
- U. Apple TV uygulaması
- V. Apple ile Giriş Yap

IV. Sık Sorulan Sorular

I. Genel Bilgiler

Apple; mobil haberleşme ve medya aygıtları, kişisel bilgisayarlar, taşınabilir dijital müzik çalarlar tasarlar, üretir ve pazarlar. Aynı zamanda çeşitli ilgili yazılımların, servislerin, çevre birimlerinin, ağ çözümlerinin ve üçüncü taraf dijital içerik ve uygulamalarının satışını yapar. Apple'ın ürün ve hizmetleri arasında Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, tüketiciye yönelik ve profesyonel yazılım uygulamaları portföyü, iOS ve macOS X işletim sistemleri, iCloud ve çeşitli aksesuar, servis ve destek teklifleri yer alır. Ayrıca Apple; Apple Music, App Store, Apple Books ve Mac App Store aracılığıyla dijital içerik ve uygulamalar satar ve sağlar. Apple belirli bir hizmet teklifi için müşteri bilgilerini Apple [gizlilik politikasına](#) ve geçerli [hizmet kullanım şartlarına](#) uygun olarak tutar. Apple, Apple ürünlerini ve hizmetlerini kullanan müşterilerin ("Apple müşterileri") gizliliğini korumayı taahhüt eder. Bu doğrultuda, Apple müşterileri ile ilgili bilgiler, yasalarda öngörülen acil durumlar dışında, geçerli bir yasal süreç söz konusu olmadığı sürece açıklanmaz.

Bu Yönergelerde yer alan bilgiler, Apple'ın ABD dışındaki devlet kurumları ve emniyet teşkilatlarına elektronik bilgileri ifşa etmesi gereken yasal süreçlerle ilgili olarak ABD dışındaki devlet kurumları ve emniyet teşkilatlarına nasıl bilgi sağlanacağını belirlemek üzere tasarlanmıştır. Bu Yönergeler, yasal tavsiye vermek üzere tasarlanmamıştır. Bu Yönergelerde yer alan sık sorulan sorular ("SSS") bölümü, Apple'a yaygın olarak iletilen bazı sorulara yanıt vermek amacıyla hazırlanmıştır. Bu Yönergeler ve SSS bölümü, ortaya çıkabilecek tüm olası durumları kapsamaz.

Başka sorularınız varsa lütfen lawenforcement@apple.com ile iletişime geçin.

Yukarıdaki posta kutusu yalnızca devlet kurumları ve emniyet teşkilatları personelinin kullanımı içindir. Bu posta kutusuna bir e-posta göndermeyi seçmeniz halinde bu e-posta, devlet kurumlarına veya emniyet teşkilatlarına ait resmi ve geçerli e-posta adresinden gönderilmelidir.

Apple'a gönderilen yasal taleplerde, belirli bir Apple aygıtı veya müşterisi ve Apple'ın o müşteriye sağlıyor olabileceği belirli servisler hakkında bilgi isteniyor olmalıdır. Apple, Apple aygıtları veya müşterileri ile ilgili talep edilen bilgileri, bu bilgilere veri saklama politikaları çerçevesinde hâlâ sahip olduğu sürece sağlayabilir. Apple, verileri aşağıdaki belirli "Alınabilecek Bilgiler" bölümlerinde belirtilen şekilde saklar. Diğer tüm veriler [gizlilik politikamızda](#) belirtilen amaçları yerine getirmek için gerekli olan süre boyunca saklanır. Devlet kurumları ve emniyet teşkilatları; belirsiz, uygunsuz ya da aşırı geniş bir talebe karşılık olarak yanlış yorumlama, itiraz, karşı çıkma ve/veya ret içeren yanıtlardan kaçınmak için, taleplerini mümkün olduğunca sınırlı ve spesifik şekilde düzenlemelidir. Acil durumlar (aşağıda Acil Talepler bölümünde tanımlanmıştır) dışında, ABD dışındaki devlet kurumları ve emniyet teşkilatlarından gelen tüm içerik talepleri, ABD Elektronik Haberleşmenin Gizliliği Kanunu (ECPA) dahil olmak üzere geçerli yasalara uygun olmalıdır. Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Yasası ("CLOUD Yasası Anlaşması") uyarınca, Karşılıklı Adli Yardımlaşma Anlaşması veya bir Yürütme Anlaşması kapsamındaki talepler ECPA ile uyumludur. Apple, müşteriyle ilgili içeriği, müşterinin hesabında bulunduğu haliyle, yalnızca yasal olarak geçerli bir sürece cevaben sağlar.

Bu Yönergelerdeki hiçbir husus, Apple'a karşı uygulanabilir herhangi bir hak oluşturmayı amaçlamaz ve Apple'ın politikaları gelecekte devlet kurumlarına veya emniyet teşkilatlarına herhangi bir bildirimde bulunmaksızın güncellenebilir ya da değiştirilebilir.

II. Apple'a Gönderilen Yasal Talepler

A. Devlet Kurumları ve Emniyet Teşkilatlarının Bilgi Talepleri

Apple, devlet kurumlarından veya emniyet teşkilatlarından e-posta yoluyla gelen yasal olarak geçerli bilgi taleplerini, talepte bulunan devlet kurumunun ya da emniyet teşkilatının resmi e-posta adresinden iletilmeleri koşuluyla kabul eder. Apple'dan bilgi talebinde bulunan ABD dışındaki devlet kurumları ve emniyet teşkilatı personeli, bir [Devlet Kurumları ve Emniyet Teşkilatları Bilgi Talebi](#) şablonunu doldurmalı ve bunu doğrudan devlet kurumunun veya emniyet teşkilatlarının e-posta adresini kullanarak lawenforcement@apple.com adresine iletmelidir.

Yukarıdaki posta kutusu yalnızca devlet kurumları ve emniyet teşkilatları personelinin kullanımı içindir. Taleplerin Aygıt Seri/IMEI numaraları, Apple ID, E-posta adresleri veya Fatura/Sipariş numaraları gibi 5 ya da daha fazla tanımlayıcı içerdiği durumlarda bu talepler, düzenlenebilir bir biçimde (ör. Numbers, Excel, Pages veya Word belgesi) iletilmelidir. Bu tür tanımlayıcılar genellikle aygıtlar, hesaplar veya finansal işlemlerle ilgili bilgileri aramak için gereklidir.

Lütfen Dikkat: Apple, sistem güvenlik standartları nedeniyle, yasal talepleri veya ilgili belgeleri e-postalarda gönderilen bağlantılardan indirmeyecektir.

Apple'ın, emniyet teşkilatlarından gelen bir talebe cevaben müşteri bilgilerini ifşa etmesi için, talepte bulunan yetkilinin, emniyet teşkilatlarının Apple gibi bir Veri Denetleyicisinden kişisel veriler şeklinde kanıt niteliğindeki bilgileri toplamasına yetki veren yasal dayanağı belirtmesi gerekir. Apple'ın yasal yönden geçerli olarak kabul ettiği taleplere ilişkin örnekler: Production Orders (Avustralya, Kanada, Yeni Zelanda), lettres de réquisition ou commissions rogatoires (Fransa), Solicitud Datos (İspanya), Ordem Judicial (Brezilya), Auskunftsercukun (Almanya), Obligation de dépôt (İsviçre), 個人情報の開示依頼 (Japonya), Personal Data Request, Orders, Warrants and Communications Data Authorisations (Birleşik Krallık) ile eş değer mahkeme kararları ve/veya diğer ülkelerden gelen talepler.

B. Devlet Kurumları ve Emniyet Teşkilatlarının Bilgi Taleplerini Yönetme ve Cevaplama

Apple, tüm talepler için geçerli bir yasal dayanak bulunduğundan emin olmak üzere tüm yasal talepleri dikkatle inceler ve yasal olarak geçerli taleplere uyar. Apple, geçerli bir yasal dayanak bulunmadığını veya bir talebin belirsiz, uygunsuz ya da aşırı kapsamlı olduğunu belirlediği durumlarda, söz konusu talebe itiraz eder, karşı çıkar veya bunu reddeder.

Apple, işleme amaçları ve sistem sınırlamaları nedeniyle 25'ten fazla hesap tanımlayıcı içeren yasal talepleri kabul edemez. Emniyet teşkilatları 25'ten fazla hesap tanımlayıcı içeren yasal talepler gönderirse Apple, bunlardan ilk 25'ine yanıt verir ve emniyet teşkilatlarının herhangi bir ek tanımlayıcı için yeni bir yasal talep göndermesi gerekir.

C. Koruma Talepleri

Acil durumlar (aşağıda Acil Talepler bölümünde tanımlanmıştır) dışında, ABD dışındaki devlet kurumları ve emniyet teşkilatlarından gelen tüm içerik talepleri, ABD Elektronik Haberleşmenin Gizliliği Kanunu (ECPA) dahil olmak üzere geçerli yasalara uygun olmalıdır. A Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Yasası ("CLOUD Yasası Anlaşması") uyarınca, Karşılıklı Adli Yardımlaşma Anlaşması veya bir Yürütme Anlaşması kapsamındaki talepler ECPA ile uyumludur. ECPA ile uyumlu talepten önce gönderilecek verileri koruma talebi, e-posta yoluyla lawenforcement@apple.com adresine iletilmelidir.

Koruma talepleri, ilgili Apple ID/hesap e-posta adresini ya da söz konusu Apple hesabı müşterisinin

tam adını **ve** telefon numarasını ve/veya tam adını **ve** fiziksel adresini içermelidir. Koruma talebi alındığında Apple, talep anında mevcut olan müşteri verilerini bir kereye mahsus olmak üzere 90 gün boyunca saklar. Bu 90 günlük süre sona erdikten sonra koruma işlemi, depolama sunucusundan otomatik olarak kaldırılır. Bununla birlikte, yenilenen bir talep alınması durumunda bu süre 90 gün daha uzatılabilir. Aynı hesap için ikiden fazla koruma talebinde bulunulması halinde ikinci talep, yeni veriler için ayrı bir koruma talebi olarak değil, asıl koruma süresinin uzatılmasına yönelik bir talep olarak değerlendirilir.

D. Acil Talepler

Apple; bireylerin yaşamına/güvenliğine, bir Devletin güvenliğine veya kritik altyapı/tesislerin güvenliğine yönelik yakın ve ciddi tehditler içeren durumlarla ilgili olan talepleri acil talep olarak değerlendirir.

Talepte bulunan devlet kurumu veya emniyet teşkilatı yetkilisi, talebinin yukarıdaki kriterlerden bir ya da daha fazlasını içeren acil durumlarla ilgili olduğuna dair tatmin edici bir doğrulama sağlarsa Apple, bu tür bir talebi acil durum temelinde inceler.

Talepte bulunan devlet kurumu veya emniyet teşkilatı yetkilisi, acil durumlarda Apple'ın bilgileri gönüllü olarak ifşa etmesini talep etmek için, [Devlet Kurumları ve Emniyet Teşkilatları Acil Bilgi Talep formunu](#) doldurarak doğrudan devlet kurumuna veya emniyet teşkilatına ait resmi e-posta adresi üzerinden, konu başlığına "Acil Talep" yazarak exigent@apple.com adresine göndermelidir.

Devlet kurumu veya emniyet teşkilatının, Devlet Kurumları ve Emniyet Teşkilatları Acil Bilgi Talebine yanıt olarak müşteri verilerini istediği durumlarda Apple, söz konusu bilgi talebini gönderen devlet kurumunun ya da emniyet teşkilatının yetkili yöneticisi ile irtibat kurarak acil durum talebinin meşru olduğunu doğrulamasını isteyebilir. Devlet Kurumları ve Emniyet Teşkilatları Acil Bilgi Talebini gönderen devlet kurumu veya emniyet teşkilatı yetkilisi, göndermiş olduğu talepte yetkili yöneticinin iletişim bilgilerini sağlamalıdır.

Devlet kurumları veya emniyet teşkilatlarının acil bir soruşturma için Apple'a ulaşması gerekiyorsa lütfen 001 408 974 2095 numaralı telefondan Apple'ın Küresel Güvenlik Operasyonları Merkezi (GSOC) ile iletişime geçin. Bu telefon numarasında birden fazla dil desteği sunulmaktadır.

E. Hesap Kısıtlama/Silme Talepleri

Devlet kurumu veya emniyet teşkilatları Apple'dan bir müşterinin Apple ID'sini kısıtlamasını/silmesini talep ederse Apple, ilgili hesabın hukuka aykırı olarak kullanıldığını gösteren bir mahkeme emri veya eşdeğer bir iç hukuk süreci bildirimi (genellikle bir mahkumiyet kararı ya da tutuklama emri) sunulmasını şart koşar.

Apple, her talep için geçerli bir yasal dayanak bulunduğundan emin olmak amacıyla, devlet kurumlarından ve emniyet teşkilatlarından gelen tüm talepleri dikkatle inceler. Apple'ın geçerli bir yasal dayanak bulunmadığını veya mahkeme kararının, kısıtlanacak/silinecek hesabın yasa dışı bir şekilde kullanıldığını göstermediğini belirttiği durumda Apple, bu talebi reddedecek/talebe itiraz edecektir.

Apple, devlet kurumlarından veya emniyet teşkilatlarından kısıtlanacak/silinecek hesabın hukuka aykırı şekilde kullanıldığını gösteren tatmin edici bir mahkeme emri ya da eşdeğer bir iç hukuk süreci bildirimi (genellikle bir mahkumiyet kararı veya tutuklama emri) alırsa mahkeme kararına uygun olarak hesabı kısıtlamak/silmek için gerekli işlemleri yapar ve talepte bulunan kurumu da bu doğrultuda bilgilendirir.

F. Müşterinin Bilgilendirilmesi

Apple; bildirimde bulunmanın geçerli yasal talepte, Apple'ın aldığı bir mahkeme kararında veya geçerli yasalarda açıkça yasaklandığı durumlar, Apple'ın tamamen kendi takdirine bağlı olarak bildirimde bulunmanın kimliği belirlenebilir bir kişi için yaralanma ya da ölüm riski oluşturduğuna inandığı durumlar, olayın çocuğu tehlikeye atma ile ilgili olduğu durumlar veya bildirimin olayın temelindeki koşullar için geçerli olmadığı durumlar haricinde, devlet kurumları ya da emniyet teşkilatlarından gelen geçerli bir yasal talep doğrultusunda Apple hesap bilgileri istenen müşterileri bu konuda bilgilendirecektir.

90 gün sonra Apple, bildirimde bulunmanın mahkeme kararında veya yürürlükteki yasalarda yasaklandığı durumlar ya da Apple'ın tamamen kendi takdirine bağlı olarak bildirimde bulunmanın kimliği belirlenebilir bir kişi veya kişi grubu için yaralanma ya da ölüm riski oluşturabileceğine veya olayın çocukları tehlikeye attığına inandığı durumlar dışında, acil durum ifşaları için gecikmeli bildirimde bulunacaktır. Apple, tamamen kendi takdirine bağlı olarak, bildirimde bulunmanın kimliği belirlenebilir bir kişi veya kişi grubu için yaralanma ya da ölüm riski oluşturabileceğine veya olayın çocuğun tehlikeye atılmasıyla ilgili olduğu durumlar ya da bildirimin olayın temelindeki koşullar için geçerli olmadığı durumlar haricinde, bir mahkeme kararında belirtilen ifşa etmeme süresi sona erdikten sonra gecikmeli bildirimde bulunacaktır.

Apple; bildirimde bulunmanın ilgili yasal süreçte, Apple'a ulaşan bir mahkeme kararında veya geçerli yasalarda yasaklandığı, olayın çocuğun tehlikeye atılmasıyla ilgili olduğu, Apple'ın tamamen kendi takdirine bağlı olarak bildirimde bulunmanın kimliği belirlenebilir bir kişi ya da bir grup kişi için yaralanma veya ölüm riski oluşturduğuna makul ölçüde inandığı ya da bildirimin olayın temelindeki koşullar için geçerli olmadığı durumlar haricinde, kısıtlanacak/silinecek hesabın hukuka aykırı kullanıldığını gösteren bir mahkeme kararı (genellikle mahkumiyet kararı veya tutuklama emri) alması ya da söz konusu hesabın Apple'ın hizmet şartlarını ihlal etmesi nedeniyle Apple hesaplarının kısıtlanması/silinmesi durumunda müşterilerini bilgilendirecektir.

III. Apple'dan Alınabilecek Bilgiler

Bu bölüm, işbu Yönergelerin yayınlandığı tarihte Apple'dan alınabilecek genel bilgi türlerini kapsar.

A. Aygıt Kaydı

Müşteriler, iOS 8 ve macOS Sierra 10.12'den önceki bir Apple aygıtını kaydederken Apple'a ad, adres, e-posta adresi ve telefon numarası gibi temel kayıt bilgilerini veya müşteri bilgilerini sağlar. Apple bu bilgilerin doğruluğunu onaylamaz; bu bilgiler doğru olmayabilir ya da aygıt sahibini yansıtmayabilir. Müşteri, aygıtı bir iCloud Apple Kimliği ile ilişkilendirdiğinde, iOS 8 ve sonraki bir sürümün yüklü olduğu aygıtlar ile macOS Sierra 10.12 ve sonraki bir sürümün yüklü olduğu Mac'lerin kayıt bilgileri alınır. Bu bilgiler doğru olmayabilir veya aygıtın sahibini yansıtmayabilir. Kayıt talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Apple aygıt seri numaralarının "O" veya "I" harflerini içermediğini ve Apple'ın, bunun yerine seri numaralarında 0 (sıfır) ve 1 (bir) rakamlarını kullandığını lütfen unutmayın. "O" veya "I" harfini içeren seri numarası için gönderilen talepler sonuç vermez. Yasal bir talebin 5 veya daha fazla seri numarası içerdiği durumlarda, Apple bu seri numaralarının düzenlenebilir elektronik biçimde de (ör. Numbers, Excel, Pages veya Word belgesi) gönderilmesini ister.

B. Müşteri Hizmetleri Kayıtları

Müşterilerin bir aygıt veya hizmetle ilgili olarak Apple müşteri hizmetleriyle olan iletişimleri Apple'dan alınabilir. Bu bilgiler, belirli bir Apple aygıtı veya hizmetiyle ilgili olarak müşterilerle yapılan destek etkileşimlerinin kayıtlarını içerebilir. Ek olarak aygıt, garanti ve onarım ile ilgili bilgiler de alınabilir. Varsa bu bilgiler, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

C. Apple Medya Hizmetleri

App Store, Apple Music, Apple TV uygulaması, Apple Podcasts ve Apple Books ("Apple Medya Hizmetleri"); uygulamaları, dijital müzik ve videoları düzenlemek, oynatmak ve içerik yayımlamak için müşterilerin kullandığı yazılım uygulamalarıdır. Apple Medya Hizmetleri ayrıca müşterilerin bilgisayarlarına ve iOS aygıtlarına indirebilecekleri içerik sağlar. Müşteri bir Apple hesabı açtığında ad, fiziksel adres, e-posta adresi ve telefon numarası gibi temel müşteri bilgilerini sağlayabilir. Ek olarak, Apple Medya Hizmetleri satın alma/indirme işlemleri ve bağlantılarının yanı sıra güncelleme/yeniden indirme bağlantıları ile ilgili bilgiler de alınabilir. IP adresi bilgileri en son 18 ay ile sınırlı olabilir. Varsa Apple Medya Hizmeti müşteri bilgileri ve IP adresleriyle bağlantı günlükleri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Apple Medya Hizmeti verilerine yönelik talepler, Apple aygıt tanımlayıcısını (seri numarası, IMEI, MEID veya GUID) ya da ilgili Apple ID/hesap e-posta adresini içermelidir. Apple ID/hesap e-posta adresi bilinmiyorsa söz konusu Apple Medya Hizmeti müşteri hesabının sahibini tanımlamak için Apple Medya Hizmeti müşteri bilgilerinin, tam adı **ve** telefon numarası ve/veya tam adı **ve** fiziksel adresi içerecek şekilde Apple'a sağlanması gerekir. Devlet kurumu veya emniyet teşkilatı yetkilileri, Apple Medya Hizmeti satın alımlarıyla ilişkili geçerli bir Apple Medya Hizmeti sipariş numarası ya da eksiksiz bir banka veya kredi kartı numarası da sağlayabilir. Bu parametrelerle birlikte müşteri adı da sağlanabilir, ancak tek başına müşteri adı, bilgi almak için yeterli değildir.

Lütfen Dikkat: Yasal talebinizin tüm kredi/banka kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, örneğin Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

D. Apple Store İşlemleri

Satış Noktası işlemleri, Apple Store'larda gerçekleşen nakit, kredi/banka kartı veya hediye kartı işlemleridir. Satış Noktası kayıtlarına yönelik talepler, kullanılan kredi/banka kartı numarasının tamamını içermelidir. Ayrıca işlem tarihi ve saati, tutar ve satın alınan ürünler gibi ek bilgiler de sağlanabilir. Varsa belirli bir satın alma işlemiyle ilişkili kartın türü, alıcının adı, e-posta adresi, işlem tarihi/saati, işlem tutarı ve mağazanın konumu ile ilgili bilgiler, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Makbuzların mükerrer kopyalarına yönelik talepler, satın alımlarla ilişkili mağaza işlem numarasını içermelidir. Varsa bu bilgiler, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Lütfen Dikkat: Yasal talebinizin tüm kredi/banka kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ör. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

E. Apple.com Siparişleri

Apple, Apple.com'dan verilen online siparişlerle ilgili bilgileri saklar. Bu bilgiler; satın alan kişinin adını, nakliye adresini, telefon numarasını, e-posta adresini, satın alınan ürünleri, satın alma tutarını ve satın alma işleminin IP adresini içerebilir. Apple.com'dan verilen online siparişlerle ilgili bilgi taleplerinde, kredi/banka kartı numarasının tamamına veya sipariş numarasına ya da satın alınan ürünün seri numarasına yer verilmelidir. Bu parametrelerle birlikte müşteri adı da sağlanabilir, ancak tek başına müşteri adı, bilgi almak için yeterli değildir. Alternatif olarak, Apple.com'dan verilen siparişlerle ilgili bilgi taleplerinde, ilgili Apple Kimliği/hesap e-posta adresi de sağlanabilir. Apple ID/hesap e-posta adresi bilinmiyorsa Apple, söz konusu Apple hesabını tanımlamak için müşteri bilgilerinin, tam adı **ve** telefon numarasını ve/veya tam adı **ve** fiziksel adresi içerecek şekilde sağlanmasını şart koşar. Mümkünse Apple.com'dan verilen online siparişler için satın alma bilgileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli olan bir talepte alınabilir.

Lütfen Dikkat: Yasal talebinizin tüm kredi/banka kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ör. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

F. Hediye Kartları

Apple Store Hediye Kartları ile App Store ve iTunes Hediye Kartlarında seri numarası bulunur. Bu seri numaraları, tasarım ve/veya veriliş tarihi gibi değişkenlere bağlı olarak birden fazla biçimde mevcuttur. Apple, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında Apple Store Hediye Kartları ile App Store ve iTunes Hediye Kartlarına ilişkin mevcut bilgileri sağlayabilir. Yasal bir talebin 5 veya daha fazla hediye kartı seri numarası içerdiği durumlarda, Apple bu hediye kartı seri numaralarının, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (ör. Numbers, Excel, Pages veya Word belgesi) içinde gönderilmesini ve şifrenin ayrı bir e-posta olarak iletilmesini ister.

i. Apple Store Hediye Kartları

Apple Store Hediye Kartları, Apple.com'dan veya Apple Store'dan yapılacak satın alımlarda kullanılabilir. Mevcut kayıtlar; hediye kartını satın alan kişinin bilgilerini (üçüncü taraf bir satıcı yerine Apple'dan satın alındıysa), ilişkili satın alma işlemlerini ve satın alınan öğeleri içerebilir. Bazı durumlarda Apple, söz konusu kartın durumuna bağlı olarak Apple Store Hediye Kartını iptal edebilir veya askıya alabilir. Varsa Apple Store Hediye Kartı bilgileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Lütfen Dikkat: Yasal talebinizin tüm Apple Store Hediye Kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ör. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

ii. App Store ve iTunes Hediye Kartları

App Store ve iTunes Hediye Kartları; Apple Music, App Store, Apple Books ve Mac App Store'da kullanılabilir. Apple, seri numarasıyla, App Store ve iTunes Hediye Kartının etkinleştirilip etkinleştirilmediğini (mağaza satış noktasından satın alınmış) veya kullanılıp kullanılmadığını (bir Apple hesabının mağaza kredisi bakiyesine eklenip eklenmediğini) belirleyebilir.

App Store ve iTunes Hediye Kartı etkinleştirildiğinde, mevcut kayıtlar mağazanın adını, konumunu, işlem tarihini ve saatini içerebilir. App Store ve iTunes Hediye Kartı kullanıldığında, mevcut kayıtlar ilgili Apple hesabı için müşteri bilgilerini, kartın etkinleştirildiği ve/veya kullanıldığı tarihi, saati ve kullanıldığı IP adresini içerebilir. Bazı durumlarda Apple, söz konusu kartın durumuna bağlı olarak App Store ve iTunes Hediye Kartını devre dışı bırakabilir. Varsa App Store ve iTunes Hediye Kartı bilgileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Lütfen Dikkat: Yasal talebinizin tüm App Store ve iTunes Hediye Kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ör. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

G. Apple Pay

Satış yerlerinde ve uygulamalarda veya online satış noktalarında yapılan Apple Pay işlemleri (ör. NFC/temassız iletişim için) müşterinin aygıtında güvenli bir şekilde doğrulanır ve satıcıya ya da satıcının ödeme işlemcisine şifreli biçimde gönderilir. İşlem güvenliği bir Apple sunucusu tarafından doğrulansa da Apple, ödemeleri işleme koymaz veya bu tür işlemleri veya Apple Pay kullanılarak yapılan satın almalarda kullanılan tüm kredi/banka kartı numaralarını saklamaz. Bu bilgilere ilgili banka, ödeme ağı veya satıcı aracılığıyla ulaşılabilir.

Apple Pay'in desteklendiği ülkeler ve bölgeler hakkında daha fazla bilgiye support.apple.com/kb/HT207957 adresinden ulaşılabilir.

Apple Store'lardan veya Apple.com üzerinden yapılan satın alımlara yönelik işlem verileri taleplerinde Apple, işlemde kullanılan Aygıt Birincil Hesap Numarası (DPAN) sağlanmasını şart koşar. DPAN 16 hanelidir ve kartı veren bankadan alınabilir. Not: DPAN, satıcı ile yapılan temassız ödeme işlemlerinde gerçek kredi/banka kartı numarası (FPAN/Finansman PAN'ı) yerine kullanılır. DPAN, ödeme işlemcisi tarafından ilgili FPAN'a dönüştürülür. Apple, ilgili DPAN bilgilerini kullanarak, satış noktası sistemi aracılığıyla uyumlu bilgileri bulmak için makul bir arama yapabilir. Varsa bu kayıtlar, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Apple, bir müşterinin Apple Pay'e eklediği kredi/banka kartı türleriyle ilgili Apple Pay bilgilerini müşteri bilgileriyle birlikte sağlayabilir. Varsa bu bilgiler, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir. Apple, bu tür bilgileri talep etmek için bir aygıt tanımlayıcısı (Apple seri numarası, SEID, IMEI veya MEID) ya da bir Apple ID/hesap e-posta adresi sağlanmasını şart koşar.

Lütfen Dikkat: Yasal talebinizin DPAN verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ör. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

H. iCloud

iCloud, Apple'ın, müşterilerin fotoğraflarına, belgelerine ve daha fazlasına tüm aygıtlarından erişmelerini sağlayan bulut hizmetidir. iCloud, müşterilerin iOS ve iPadOS aygıtlarını iCloud'a yedeklemelerine de olanak tanır. Müşteriler, iCloud hizmetiyle bir iCloud.com e-posta hesabı oluşturabilir. iCloud e-posta etki alanları @icloud.com, @me.com ve @mac.com şeklinde olabilir. Apple tarafından depolanan iCloud içeriğine ilişkin tüm veriler sunucunun bulunduğu konumda şifrelenir. Apple, şifresini çözebildiği verilere ilişkin şifreleme anahtarlarını ABD'deki veri merkezlerinde saklar. Apple, müşterinin uçtan uca şifrelenmiş verilerine ilişkin şifreleme anahtarlarını almaz veya saklamaz.

iCloud, müşteri tabanlı bir hizmettir. iCloud verilerine yönelik talepler, ilgili Apple ID/hesap e-posta adresini içermelidir. Apple ID/hesap e-posta adresi bilinmiyorsa Apple, söz konusu Apple hesabını tanımlamak için müşteri bilgilerinin, tam adı **ve** telefon numarasını ve/veya tam adı **ve** fiziksel adresi içerecek şekilde sağlanmasını şart koşar. Yalnızca bir telefon numarası veya Apple ID/hesap e-posta adresinin sağlandığı durumlarda, bu kriterlerle ilişkili doğrulanmış hesaplar için mevcut bilgiler üretilebilir.

I. Aşağıdaki bilgiler iCloud'dan edinilebilir:

I. Müşteri bilgileri

Müşteri bir iCloud hesabı oluşturduğunda Apple'a ad, fiziksel adres, e-posta adresi ve telefon numarası gibi temel müşteri bilgilerini sağlayabilir. Ayrıca, iCloud özelliği bağlantılarıyla ilgili bilgiler de alınabilir. iCloud, Varsa müşteri bilgileri ve IP adresleriyle birlikte bağlantı günlükleri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir. Bağlantı günlükleri 25 güne kadar saklanır.

II. Posta Günlükleri

Posta günlükleri; saat, tarih, gönderenin e-posta adresleri ve alıcının e-posta adresleri gibi gelen ve giden iletişimlerin kayıtlarını içerir. iCloud posta günlükleri en fazla 25 gün saklanır ve mevcut olması halinde, talep sahibinin ülkesinde yasal olarak geçerli bir talep üzerine elde edilebilir.

III. E-posta İçeriği ve Diğer iCloud İçeriği, Fotoğraf Yayınım, iCloud Fotoğraf Kitaplığı, iCloud Drive, Kişiler, Takvimler, Yer İmleri, Safari Tarama Geçmişi, Haritalar Arama Geçmişi, Mesajlar, iOS Aygıt Yedeklemeleri

iCloud, müşterinin hesabı etkin olduğu sürece müşterinin hesapta tutmayı seçtiği hizmetlere ilişkin içeriği saklar. Apple, Apple'ın sunucularından silinmiş olan içerikleri saklamaz. iCloud içeriği; e-posta, depolanan fotoğraflar, belgeler, kişiler, takvimler, yer imleri, Safari gezinme geçmişi, Harita Arama Geçmişi, Mesajlar ve iOS aygıt yedeklemelerini içerebilir. iOS aygıt yedeklemelerinin içinde; Film Rulosu, aygıt ayarları, uygulama verileri, iMessage, İş Yeriyle Sohbet, SMS ve MMS

mesajları ile sesli mesajlar yer alan fotoğraflar ve videolar bulunabilir. Apple tarafından depolanan iCloud içeriğine ilişkin tüm veriler sunucunun bulunduğu konumda şifrelenir. Apple, şifresini çözebildiği verilere ilişkin şifreleme anahtarlarını ABD'deki veri merkezlerinde saklar. Apple, müşterinin uçtan uca şifrelenmiş verilerine ilişkin şifreleme anahtarlarını almaz veya saklamaz.

Acil durumlar (yukarıda Acil Talepler bölümünde tanımlanmıştır) dışında, ABD dışındaki devlet kurumlarından ve emniyet teşkilatlarından gelen tüm içerik talepleri, ABD Elektronik Haberleşmenin Gizliliği Kanunu (ECPA) dahil olmak üzere geçerli yasalara uygun olmalıdır. Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Yasası ("CLOUD Yasası Anlaşması") uyarınca, Karşılıklı Adli Yardımlaşma Anlaşması veya bir Yürütme Anlaşması kapsamındaki talepler ECPA ile uyumludur. Apple, müşteriyle ilgili içeriği, müşterinin hesabında bulunduğu haliyle, yalnızca yasal olarak geçerli bir talebe cevaben sağlar.

II. İleri Düzey Veri Koruma

iCloud için İleri Düzey Veri Koruma, iCloud verilerinin Apple'ın en ileri düzey veri güvenliğiyle korunması için uçtan uca şifreleme kullanılan bir özelliktir. iCloud için İleri Düzey Veri Koruma özelliğini etkinleştiren kullanıcılar için sınırlı iCloud verisi söz konusu olabilir. İleri Düzey Veri Koruma hakkında daha fazla bilgiyi support.apple.com/guide/security/advanced-data-protection-for-icloud-sec973254c5f/web ve support.apple.com/tr-tr/HT212520 web adreslerinden alabilirsiniz.

Bir kullanıcı iCloud için İleri Düzey Veri Koruması'nı etkinleştirmişse aşağıdaki bilgileri iCloud'dan edinilebilir:

a. Müşteri Bilgileri

Müşteri bir iCloud hesabı oluşturduğunda Apple'a ad, fiziksel adres, e-posta adresi ve telefon numarası gibi temel müşteri bilgilerini sağlayabilir. Ayrıca, iCloud özellik bağlantılarıyla ilgili bilgiler de sunulabilir. Varsa iCloud müşteri bilgileri ve IP adresleriyle birlikte bağlantı günlükleri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir. Bağlantı günlükleri 25 güne kadar saklanır.

b. Posta Günlükleri

Posta günlükleri; saat, tarih, gönderenin e-posta adresleri ve alıcının e-posta adresleri gibi gelen ve giden iletişimlerin kayıtlarını içerir. iCloud posta günlükleri en fazla 25 gün saklanır ve mevcut olması halinde, talep sahibinin ülkesinde yasal olarak geçerli bir talep üzerine elde edilebilir.

b. c. E-posta İçerikleri ve Diğer iCloud İçerikleri

iCloud, İleri Düzey Veri Koruma'yı etkinleştiren kullanıcılar için müşterinin hesabı etkin durumdayken müşterinin hesapta bulundurmaya seçtiği e-posta, kişiler ve takvimlerle ilgili içerikleri saklar. Bu veriler, müşterinin hesabında olduğu şekliyle, talep sahibinin bulunduğu ülkede düzenlenmiş yasal olarak geçerli bir taleple karşılığında sağlanabilir. Bu sınırlı veriler, Apple tarafından saklanır ve ayrıca sunucu konumunda şifrelenir. Apple, şifresini çözebildiği verilere ilişkin şifreleme anahtarlarını ABD'deki veri merkezlerinde saklar. Apple, müşterinin uçtan uca şifrelenmiş verilerine ilişkin şifreleme anahtarlarını almaz veya saklamaz.

İleri Düzey Veri Koruması'nda uçtan uca şifreleme kullanılır. Apple; Fotoğraflar, iCloud Drive, Yedekleme, Notlar ve Safari Yer İmleri gibi belirli iCloud içeriklerinin şifresini çözemez. Bazı durumlarda Apple, söz konusu iCloud hizmetleriyle ilgili olarak, varsa talepte bulunan tarafın ülkesinde düzenlenmiş yasal olarak geçerli uygun bir talep

karşılığında edinilebilecek sınırlı bilgileri saklayabilir.

III. iCloud Özel Geçişi

iCloud Özel Geçişi, iCloud+ aboneliği kapsamında sunulan bir internet gizlilik hizmetidir. Özel Geçiş, kullanıcıların Safari ile web'de dolaşma bilgilerini, DNS (Alan Adı Yeri) çözümleme sorgularını ve şifrelenmemiş http uygulama trafiğini korur. Bunun için kullanıcıların iCloud+ aboneliğinin olması ve iCloud Özel Geçişi'ni kullanabilmesi için aygıtlarında iOS 15, iPadOS 15 veya macOS Monterey (macOS 12) ya da daha yeni bir sürümün yüklü olması gerekir. Özel Geçiş hakkında daha fazla bilgiyi support.apple.com/tr-tr/HT212614 ve www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF web adreslerinden alabilirsiniz.

Özel Geçiş etkinleştirildiğinde, kullanıcıların internette gezinme istekleri iki ayrı güvenli internet geçişi aracılığıyla gönderilir. Kullanıcının IP adresini, kullanıcının ağ sağlayıcısı ve Apple tarafından yönetilen ilk geçiş görebilir. Kullanıcının DNS kayıtları şifrelenir. Böylece taraflardan hiçbirisi, kullanıcının ziyaret etmeye çalıştığı web sitesinin adresini göremez. Bir üçüncü taraf içerik sağlayıcısı tarafından yönetilen ikinci geçiş, geçici bir IP adresi oluşturur, kullanıcının istediği web sitesi adının şifresini çözer ve kullanıcıyı siteye bağlar. Özel Geçiş, bağlanmakta olan istemcinin bir iPhone, iPad veya Mac olduğunu doğrular. Özel Geçiş, kullanıcının orijinal IP adresini, hizmet tarafından kullanılan IP adresi aralığından atanan bir adresle değiştirir. Atanan geçiş IP adresi, aynı alandaki birden fazla Özel Geçiş kullanıcısı arasında paylaşılabılır.

Kullanıcıların web'de dolaşma isteklerinin Özel Geçiş özelliğini kullandığı durumlarda Apple, Özel Geçiş IP adreslerinden kullanıcının istemci IP adresini veya ilgili kullanıcı hesabını belirleyemez. Apple'ın, Özel Geçiş IP adresiyle ilişkili Apple Kimliği ile ilgili olarak sunacağı hiçbir bilgi yoktur.

Not: iCloud Özel Geçişi her ülkede veya bölgede kullanılamaz. Kullanıcılar Özel Geçiş özelliğini etkinleştirdiğinde ve bu özelliğin kullanılmadığı yerlere seyahat ettiğinde, Özel Geçiş otomatik olarak kapanır; kullanıcılar bu özelliğin desteklendiği bir ülke veya bölgeye yeniden girdiklerinde yeniden açılır.

I. Bul

Bul; bir iCloud müşterisinin kaybettiği ya da bulamadığı iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac, AirTag'ini bulmasını ve/veya aygıtı kayıp moduna alma, kilitleme ya da silme dahil olmak üzere belirli eylemleri gerçekleştirmesini sağlayan, kullanıcı tarafından etkinleştirilen bir özelliktir. Bu hizmet hakkında daha fazla bilgiyi www.apple.com/tr/icloud/find-my/ adresinde bulabilirsiniz.

Müşterinin aygıtını kaybettiği durumlarda Bul özelliğinin kullanılabilmesi için, bu özelliğin kaybolmadan önce söz konusu aygıtta etkinleştirilmiş olması gerekir. Bir aygıttaki Bul özelliği, uzaktan veya aygıt kaybolduktan sonra ya da bir devlet kurumunun veya emniyet teşkilatının talebi üzerine etkinleştirilemez. Aygıt konum hizmetlerine ilişkin bilgiler aygıtların kendisinde saklanır ve Apple bu bilgileri herhangi bir aygıttan alamaz. Bul özelliği aracılığıyla bulunan bir aygıtın konum hizmetleri bilgileri müşteriye yönelik olup Apple, hizmet aracılığıyla iletilen harita veya uyarı içeriğine sahip değildir. Şu destek bağlantısı, bir iOS aygıtının kaybolması veya çalınması durumuna ilişkin bilgiler ve bu gibi durumlarda müşteri tarafından uygulanabilecek adımları sağlar: support.apple.com/tr-tr/HT201472.

Bul bağlantı günlükleri 25 güne kadar kullanılabilir ve varsa talepte bulunan tarafın ülkesinde yasal

olarak geçerli, uygun bir talep karşılığında alınabilir. Varsa, bir aygıt uzaktan kilitleme veya silme talepleri doğrultusunda, gerçekleştirilen Bul işlem etkinliği, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

J. AirTag ve Bul Ağı Aksesuar Programı

iPhone, iPad, iPod touch ve Mac'teki Bul uygulaması, müşterilerin AirTag ekleyerek veya Bul Ağı Aksesuar Programı'nın parçası olan bir ürünü kullanarak kişisel nesnelerini bulmalarını kolaylaştırır.

AirTag ile iOS 14.5 ve macOS 11.3 veya sonraki sürümlerde, Bul uygulamasını kullanarak müşterilere, kayıp kişisel nesnelerini (anahtarlar, sırt çantası, valiz vb.) bulma desteği sağlanabilir. Bir ses çalabilmek veya uyumlu iPhone modellerinde Tam Konum Bulma özelliğini kullanmak için AirTag, eşleştirilen iPhone, iPad veya iPod touch aygıtının Bluetooth kapsama alanında olmalıdır. Sahibinin yakınında olmayan bir AirTag, dünyanın dört bir yanında yüz milyonlarca Apple aygıtından oluşan Bul ağındaki bir aygıtın menzili içindeyse söz konusu AirTag'in yaklaşık konumu sağlanabilir. Daha fazla bilgiyi şu adreste bulabilirsiniz: support.apple.com/tr-tr/HT212227 ve support.apple.com/tr-tr/HT210967.

Bul ağı aksesuar programı, Bul ağını üçüncü taraf aygıt üreticisi ürünlerine (bisikletler, kulaklıklar vb.) açarak hizmetten yararlanmayı sağlar. Böylece müşteriler, iOS 14.3 ve macOS 11.1 veya sonraki sürümlerde Bul uygulamasıyla desteklenen üçüncü taraf ürünlerini bulabilir.

AirTag veya desteklenen üçüncü taraf ürünlerini Bul uygulamasında Nesneler sekmesine eklemek için müşterilerin bir Apple ID'sinin olması, Bul özelliği etkinleştirilmiş olarak iCloud hesaplarında oturum açmaları ve AirTag'lerini ya da desteklenen üçüncü taraf ürünlerini Apple ID'lerine kaydetmeleri gerekir. Etkileşim uçtan uca şifrelenir ve Apple, AirTag'in veya desteklenen üçüncü taraf ürünlerinin konumunu göremez. Daha fazla bilgiye support.apple.com/tr-tr/HT211331 adresinden ulaşılabilir.

Apple, seri numarasını kullanarak, talepte bulunan tarafın ülkesinde yasal olarak geçerli uygun bir talebe cevaben, eşleştirilmiş hesap ayrıntılarını sağlayabilir. AirTag eşleştirme geçmişi 25 güne kadar kullanılabilir. Şu destek bağlantısı, AirTag seri numarası bulma hakkında bilgi sağlar: support.apple.com/tr-tr/HT211658.

Apple aygıt seri numaralarının "O" veya "I" harflerini içermediğini ve Apple'ın, bunun yerine seri numaralarında 0 (sıfır) ve 1 (bir) rakamlarını kullandığını lütfen unutmayın. "O" veya "I" harfini içeren seri numarası için gönderilen talepler sonuç vermez. Yasal bir talebin 5 veya daha fazla seri numarası içerdiği durumlarda, Apple bu seri numaralarının düzenlenebilir elektronik biçimde de (ör. Numbers, Excel, Pages veya Word belgesi) gönderilmesini ister.

K. Parola ile Kilitlenmiş iOS Aygıtlarından Verilerin Çıkarılması

Apple, iOS 8.0 ve sonraki bir sürümün yüklü olduğu aygıtlar için iOS aygıtı veri çıkarma işlemi gerçekleştiremez çünkü emniyet teşkilatları tarafından istenilen veriler çoğu zaman şifrelenmiş verilerdir ve Apple şifreleme anahtarına sahip değildir. Tüm iPhone 6 aygıtları ve sonraki model aygıtlar, iOS 8.0 veya sonraki bir sürüm yüklü olarak üretilmektedir.

Kaliforniya Elektronik Haberleşmenin Gizliliği Kanunu (CalECPA, Kaliforniya Ceza Kanunu Bölüm 1546-1546.4) uyarınca Apple, iOS 4'ten iOS 7'ye kadar olan sürümlerin yüklü olduğu aygıtlar için, aygıtın durumuna bağlı olarak, iOS veri çıkarma işlemleri gerçekleştirebilir. Apple'ın bu kriterleri sağlayan bir aygıt için iOS veri çıkarma işlemi gerçekleştirebilmesi için emniyet teşkilatının, CalECPA

kapsamında olası bir nedenin gösterilmesi üzerine çıkarılan bir arama izni alması gerekir. CalECPA dışında Apple, emniyet teşkilatları tarafından yürütülen bir soruşturmada üçüncü taraf olarak Apple'ın verileri çıkarmasını gerektiren yerleşik herhangi bir yasal bir merci belirlemediği.

L. IP Adresi Talebi

Apple, tanımlayıcı olarak bir IP adresi ile yasal işlem başlatmadan önce, emniyet teşkilatının söz konusu IP adresinin genel veya yönlendirici bir IP adresi olmadığını ve Operatör Düzeyinde Ağ Adresi Çevrimi'ni (CGNAT) kullanmadığını belirlemesini ve yasal işlem hizmeti süresince bunun kamuya açık olmayan bir IP adresi olduğunu onaylamasını talep eder. Ayrıca, bu taleplerde üç günü geçmeyen bir tarih kısıtlaması da bulunmalıdır. Apple, böyle bir talebe yanıt olarak, emniyet teşkilatının müteakip bir yasal işlem talebinde tanımlayıcı olarak kullanmak üzere belirli bir Apple hesabını/Apple Kimliği'ni belirlemeye çalışabileceği bağlantı günlükleri oluşturabilir (aşağıdaki bölüm III.Q'ya bakın). Varsa IP adresine dayalı Apple müşteri verileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

M. Alınabilecek Diğer Aygıt Bilgileri

MAC Adresi: Ortam Erişim Denetimi adresi (MAC adresi), fiziksel ağ segmentindeki iletişim için ağ arayüzlerine atanan benzersiz bir tanımlayıcıdır. Ağ arabirimlerine sahip herhangi bir Apple ürünü; Bluetooth, Ethernet, Wi-Fi veya FireWire gibi bir ya da daha fazla MAC adresine sahiptir. Varsa ilgili MAC adresi bilgileri, Apple'a bir seri numarası (veya iOS aygıtı için IMEI, MEID ya da UDID) sağlanarak talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

N. Apple Store CCTV Verilerine Yönelik Talepler

CCTV verileri mağazanın konumuna göre değişebilir. CCTV verileri Apple mağazasında genellikle en fazla 30 gün süreyle saklanır. Yerel yasalar dikkate alındığında bu süre, birçok yargı alanı için yirmi dört (24) saat kadar kısadır. Bu süre geçtikten sonra veriler kullanılamaz. Yalnızca CCTV verilerine yönelik talepler lawenforcement@apple.com adresine gönderilebilir. Devlet kurumları veya emniyet teşkilatları, talep edilen verilerle ilgili olarak belirli bir tarih, saat ve işlem bilgilerini sağlamalıdır.

O. Game Center

Game Center, Apple'ın sosyal oyun ağıdır. Bir müşteri veya aygıt için Game Center bağlantılarıyla ilgili bilgiler alınabilir. Varsa bağlantı günlükleri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

P. iOS Aygıt Aktivasyonu

Müşteri hücresel servis sağlayıcısı aracılığıyla iOS aygıtını etkinleştirdiğinde veya yazılımı yükselttiğinde, etkinliğe bağlı olarak servis sağlayıcısından ya da aygıttan Apple'a belirli bilgiler aktarılır. Bunlar arasında etkinliğin IP adresleri, ICCID numaraları ve diğer aygıt tanımlayıcıları yer alabilir. Varsa bu bilgiler, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

Çift SIM: Çift SIM özellikli aygıtlar için, varsa nano SIM ve/veya eSIM'e ilişkin operatör bilgileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir. eSIM, müşterilerin fiziksel nano SIM kullanmak zorunda kalmadan, operatörden hücresel planı etkinleştirmesine olanak tanıyan dijital bir SIM'dir. Daha fazla bilgiye support.apple.com/tr-tr/HT209044 adresinden ulaşılabilir.

Çin ana karası, Hong Kong ve Makao'da iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max ve iPhone XR modelleri, iki nano SIM kart ile Çift SIM özelliğine sahiptir.

Q. Bağlantı Günlükleri

Mevcut olduğu durumlarda müşterilerin veya aygıtların Apple Music, Apple TV uygulaması, Apple Podcasts, Apple Books, iCloud, Apple ID'm ve Apple Discussions gibi Apple hizmetlerine bağlantı etkinliği Apple'dan alınabilir. Varsa IP adresleriyle birlikte bu bağlantı günlükleri, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

R. Apple ID'm ve iForgot Günlükleri

Bir müşteriye ait Apple ID'm ve iForgot günlükleri Apple'dan alınabilir. Apple ID'm ve iForgot günlükleri, parola sıfırlama işlemleriyle ilgili bilgileri içerebilir. Varsa IP adresleriyle birlikte bağlantı günlükleri, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

S. FaceTime

FaceTime iletişimleri uçtan uca şifrelenir ve Apple, aygıtlar arasında geçiş halindeyken FaceTime verilerinin şifresini çözemez. Apple, FaceTime iletişimlerini engelleyemez. Apple, FaceTime arama daveti başlatıldığında FaceTime arama daveti kayıtlarını alır. Bu kayıtlar, müşteriler arasında herhangi bir iletişimin gerçekleştiği anlamına gelmez. FaceTime arama daveti günlükleri 25 güne kadar saklanır. Varsa FaceTime arama daveti günlükleri, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

T. iMessage

iMessage iletişimleri uçtan uca şifrelenir ve Apple, aygıtlar arasında geçiş halindeyken iMessage verilerinin şifresini çözemez. Apple, iMessage iletişimlerini engelleyemez ve iMessage iletişim günlüklerine sahip değildir. Apple, iMessage özelliği sorgu günlüklerine sahiptir. Bu günlükler, arama işleminin (ör. telefon numarası, e-posta adresi veya Apple ID) "iMessage özellikli" olup olmadığını belirlemek için bir aygıt uygulaması (ör. Mesajlar, Kişiler, Telefon ya da diğer aygıt uygulamaları) tarafından bir sorgunun başlatıldığını ve Apple'ın sunucularına yönlendirildiğini gösterir. iMessage özelliği, müşteriler arasında herhangi bir iletişimin gerçekleştiği anlamına gelmez. Apple, iMessage özelliği sorgu günlüklerine dayanarak herhangi bir iMessage iletişiminin gerçekten gerçekleşip gerçekleşmediğini belirleyemez. Ayrıca Apple, sorguyu başlatan gerçek uygulamayı tanımlayamaz. iMessage özelliği sorgu günlükleri, gerçekten bir iMessage etkinliği girişiminde bulunulduğunu doğrulamaz. iMessage özelliği sorgu günlükleri 25 güne kadar saklanır. Varsa iMessage özelliği sorgu günlükleri, talepte bulunan tarafın ülkesi için yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

U. Apple TV uygulaması

Apple TV uygulaması, müşterilerin Apple TV+, Apple TV Kanalları ile üçüncü taraf uygulama ve hizmetleri üzerinden TV şovlarına ve filmlere göz atması ve abone olmasının yanı sıra bunları satın almasına ve oynatmasına olanak tanır. Satın alma ve indirme geçmişine ulaşılabilir.

Apple TV uygulaması müşteri verilerine yönelik talepler, Apple aygıt tanımlayıcısını (seri numarası, IMEI,

MEID veya GUID) ya da ilgili Apple ID/hesap e-posta adresini içermelidir. Apple ID ya da hesap e-posta adresi bilinmiyorsa söz konusu müşteri hesabını tanımlamak için müşteri bilgileri, tam adı ve telefon numarası ve/veya tam adı ve fiziksel adresi içerecek şekilde Apple'a sağlanmalıdır. Devlet kurumları veya emniyet teşkilatları yetkilileri, Apple TV uygulaması satın alımlarıyla ilişkili geçerli bir Apple sipariş numarası ya da tam kredi/banka kartı numarası da sağlayabilir. Bu parametrelerle birlikte müşteri adı da sağlanabilir, ancak tek başına müşteri adı, bilgi almak için yeterli değildir.

Lütfen Dikkat: Yasal talebinizin tüm kredi/banka kartı verilerini içerdiği durumlarda, veri güvenliğini sağlamak amacıyla bu tür verilerin, lawenforcement@apple.com adresine şifre korumalı/şifreli bir belge (.PDF ve düzenlenebilir biçimde bir belge, ö. Numbers, Excel, Pages veya Word) içinde gönderilmesi ve şifrenin ayrı bir e-posta olarak iletilmesi gerekir. Buna ek olarak Apple, sistem güvenlik standartları nedeniyle, yasal talep belgelerini e-postalarda gönderilen bağlantılardan indirmeyecektir.

V. Apple ile Giriş Yap

Apple ile Giriş Yap, müşterilerin mevcut Apple ID'sini kullanarak üçüncü taraf uygulamalarına ve web sitelerine daha gizli bir şekilde giriş yapmalarını sağlar. Katılımcı uygulamalar veya web sitelerindeki Apple ile Giriş Yap düğmesi, müşterinin bir hesap oluşturmaya ve Apple ID ile giriş yapmasına olanak tanır. Müşteri, bir sosyal medya hesabı kullanmak veya formları doldurup yeni bir şifre seçmek yerine, yalnızca Apple ile Giriş Yap düğmesine dokunarak bilgilerini gözden geçirebilir ve Face ID, Touch ID ya da aygıt parolasıyla hızlı ve güvenli bir şekilde giriş yapabilir. Daha fazla bilgiye support.apple.com/tr-tr/HT210318 adresinden ulaşılabilir.

E-Postamı Gizle, Apple ile Giriş Yap kapsamında sunulan bir özelliktir. E-postaları müşterinin kişisel e-posta adresine ileten benzersiz, rastgele bir e-posta adresi oluşturmak ve paylaşmak için Apple'ın özel e-posta aktarma hizmetini kullanır. Temel müşteri bilgileri, talepte bulunan tarafın ülkesinde yasal olarak geçerli, uygun bir talep karşılığında alınabilir.

IV.Sık Sorulan Sorular

Q: Emniyet teşkilatının bilgi talebiyle ilgili sorularımı Apple'a e-posta ile gönderebilir miyim?

A: Evet, devlet kurumlarının yasal süreciyle ilgili sorularınızı veya sorgularınızı lawenforcement@apple.com adresine gönderebilirsiniz.

Q: Bir aygıtın çalışması veya kullanılması için Apple'a kayıtlı olması gerekir mi?

A: Hayır, bir aygıtın çalışması veya kullanılması için Apple'a kayıtlı olması gerekmez.

Q: Apple bana şu anda kilitli olan bir iOS aygıtının parolasını sağlayabilir mi?

A: Hayır, Apple, müşterilerin parolalarına erişemez.

Q: Kaybolan veya çalınan bir aygıtı, kaybeden kişiye iade etmeme yardım edebilir misiniz?

A: Bu gibi durumlarda lawenforcement@apple.com adresiyle iletişime geçin. Lütfen aygıtın seri numarasını (veya varsa IMEI'yi) ve diğer ilgili bilgileri e-postanıza ekleyin. Seri numarasını bulma ile ilgili bilgileri şu adresten alabilirsiniz: support.apple.com/tr-tr/HT204308.

Müşteri bilgileri mevcutsa Apple, müşteriyle iletişime geçerek aygıtı kurtarmak üzere emniyet teşkilatlarıyla irtibat kurmasına yönelik ayrıntıları sağlayacaktır. Ancak mevcut bilgilerle müşteri belirlenemezse geçerli bir yasal talep göndermeniz istenebilir.

Q: Apple, kaybolan veya çalınan aygıtların listesini tutuyor mu?

A: Hayır, Apple kaybolan veya çalınan aygıtların listesini tutmaz.

Q: Emniyet teşkilatı soruşturmayı/kamu davasını sonuçlandırdığında, edinilen bilgilerle ilgili ne yapmak gerekir?

A: Devlet kurumlarına veya emniyet teşkilatlarına sağlanan, kişisel olarak tanımlanabilir bilgileri içeren bilgi ve veriler (oluşturulan tüm kopyalar dahil), ilgili soruşturma, kamu davası ve tüm temyiz süreçleri tamamlandıktan sonra imha edilmelidir.

Q: Müşterilere, emniyet teşkilatlarından kendileriyle ilgili bilgi talebi aldığınızı bildiriyor musunuz?

A: Evet, emniyet teşkilatları, devlet kurumları ve özel sektör temsilcilerinden gelen hesap bilgisi talepleri için Apple'ın bildirim politikası geçerlidir. Apple; ifşa etmeme emri veya bildirimde bulunmayı yasaklayan geçerli yasalar olmadığı sürece ya da tamamen kendi takdirine bağlı olarak, böyle bir bildirimin toplum üyesi için ciddi yaralanma veya ölüm riski oluşturabileceğine makul olarak inandığı, olayın çocuğun tehlikeye atılmasıyla ilgili olduğu ve bildirimin olayın temelindeki gerçekler için geçerli olmadığı durumlar haricinde müşterileri ve hesap sahiplerini bilgilendirecektir.