MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler

BİLGİ NOTU

Kişisel Verileri Koruma Kurumu "Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler" Başlıklı Bir Rehber Yayımladı

Kişisel Verileri Koruma Kurumu ("**Kurum**"), 22.12.2023 tarihinde yayımlamış olduğu "Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler" başlıklı rehber ("**Rehber**") çerçevesinde aşağıdaki hususlara yer vermiştir.

A) Mobil Uygulamalar Kapsamında İşlenen Kişisel Veriler

Rehberde, çeşitli verilerin; kullanıcı deneyiminin zenginleştirilmesi, işlevsellik sağlanması, sunulan hizmetin iyileştirilmesi, pazarlama stratejileri oluşturulması ve benzeri amaçlar ile işlenebileceği belirtilmiş ve uygulamalar bakımından farklılık gösterebilecek olmakla birlikte, mobil uygulamalar aracılığıyla işlenen kişisel verilerin aşağıdaki şekilde örneklendirilebileceği ifade edilmiştir.

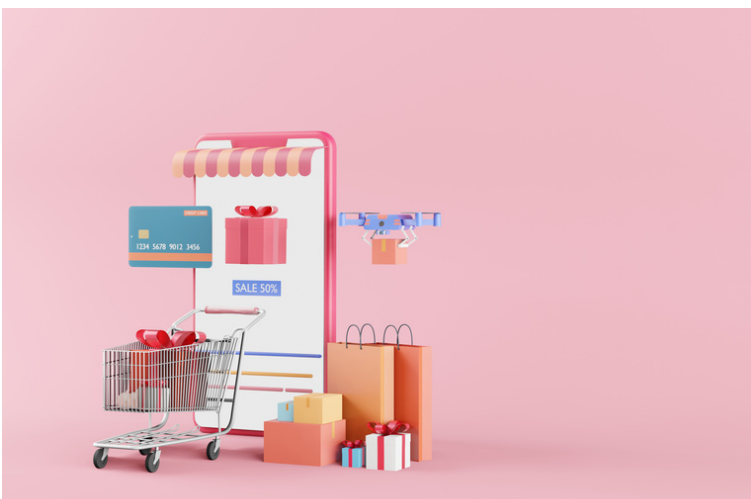
- **Kimlik bilgileri** (Ad, soyad, T.C. kimlik numarası, doğum tarihi vb.)
- **Üyelik bilgileri** (kullanıcı adı, parola vb.)
- **İletişim bilgileri** (ev adresi, telefon numarası, e-posta adresi vb.)
- **Finansal bilgiler** (IBAN, kredi kartı numarası vb.)
- **Çevrim içi tanımlayıcılar** (IP adresi, MAC adresi, IMEI ve IMSI numarası, cihazda yüklü uygulama listesi aracılığıyla parmak izi çıkarılması vb.)
- **Kullanıcı etkileşimleri** (arama geçmişi, uygulama içi satın alımlar vb.)
- **Konum bilgisi**
- **Telefon rehberi veya uygulamalardaki arkadaş listeleri**
- **Biyometrik veriler** (yüz tanıma verisi, parmak izi verisi, ses izi biyometrisi vb.)
- **Uygulamanın sağlık ile ilgili olması durumunda sağlık verileri** (kalp atış hızı, uyku düzeni vb.)
- **Cihazın kamerası ve galerisine erişim izni verilmesiyle toplanan görsel veriler**
- **Sesli komutlar veya mesajlaşma uygulamaları aracılığıyla toplanan işitsel veriler**
- **Mesajlaşma platformlarından toplanan metin verileri**

Rehber aynı zamanda, mobil uygulamalar aracılığıyla, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**") anlamında daha sıkı korumaya tabi olan özel nitelikli kişisel verilerin işlenmesinin söz konusu olabileceğini özellikle vurgulamıştır. Bu anlamda, ses tanıma uygulamaları aracılığıyla ses izi biyometrisi kullanılarak kişi hakkında biyometrik verilerin; sağlık uygulamaları aracılığıyla sağlık verilerinin (ve fotoğraf, mesaj vb. özel nitelikli kişisel veri içerebilecek olan ögelerin) elde edilebileceği gibi örneklere de yer verilmiştir.

B) Mobil Uygulamalar Kapsamında Veri Sorumlusu ve Veri İşleyen

Rehberde, mobil uygulamalar kapsamında karşılaşılan uygulama sağlayıcısı, uygulama geliştiricisi, reklam ağı, uygulama mağazası kuruluşu, işletim sistemi sağlayıcısı, kütüphane sağlayıcısı ve cihaz üreticisi gibi çeşitli aktörlerin; veri sorumlusu ve veri işleyen sıfatları, farklı örnekler ile ayrıntılı bir biçimde açıklanmıştır. Bu örnekler kısaca şu şekildedir:

- Uygulama sağlayıcısı; kullanıcılara ait kişisel verileri kendi amaçları ile kullandığı ölçüde, KVKK anlamında çoğunlukla veri sorumlusu olarak kabul edilecektir.
- Mobil uygulamalar kapsamında, birden fazla veri sorumlusu bulunması söz konusu olabilecektir. (Örneğin, üçüncü taraf bir hizmetin mobil uygulamaya entegre edilmesi hali)
- İşletim sistemi sağlayıcısı, cihazdaki mobil uygulamalar kullanıldığında verileri bir araya getirebilecek ve topladığı bu kişisel verileri kendi amaçları ile kullanabilecektir. Bu halde ise, işletim sistemi sağlayıcısının da veri sorumlusu sıfatını haiz olması mümkün olabilecektir.
- Bir diğer ihtimal ise, uygulama sağlayıcısı ve geliştiricisinin farklı kuruluşlar olması halidir. Bu doğrultuda, uygulama geliştiricisinin; kişisel veri işleme süreci bakımından sadece teknik bir rolü olması ve kendi amaçları ile kişisel veri işlememesinin güvence altına alınması kaydıyla veri işleyen olarak değerlendirilmesi mümkün olabilecektir.



C) Bireylere Yönelik Tavsiyeler

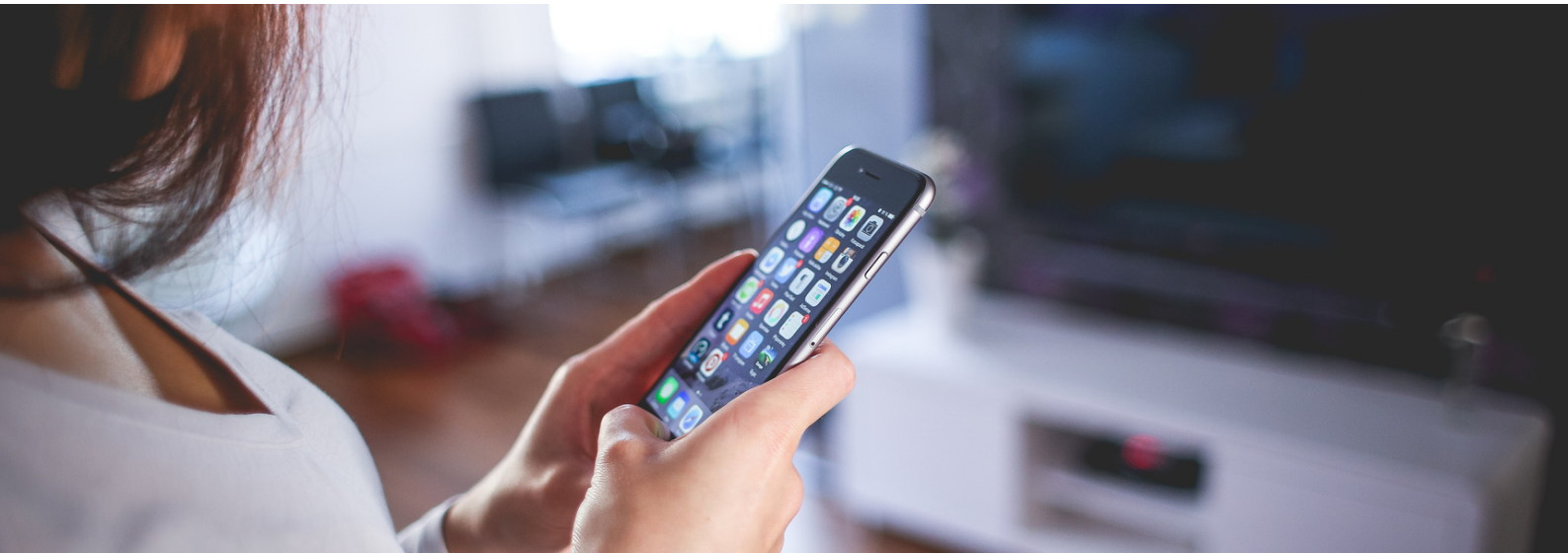
Bireylerin, mobil uygulama yüklenmeden önce ve kullanımı sürecinde dikkat etmesi gereken hususlar detaylıca ele alınmıştır. Bu hususlar kısaca şu şekildedir:

Yüklenmeden Önce:

- Mobil uygulamanın güvenilir platformlar aracılığıyla cihaza indirilmesi,
- Uygulama geliştiricisi hakkında bilgi edinilmesi, uygulama adının doğruluğundan emin olunması,
- Mobil uygulamaya ilişkin kullanıcı yorumlarının ve puanın kontrolü,
- Mobil uygulama kapsamında hangi verilere erişim izni talep edildiği ve uygulamaya ilişkin gizlilik politikasının incelenmesi.

Kullanım Sürecinde:

- Mobil uygulamanın kullanımı esnasında talep edilen izinler bakımından dikkatli olunması,
- Konum, ses ve görüntü verileri elde eden cihaz araçlarına sürekli erişim izni verilmesi yerine kullanım amacı doğrultusunda değerlendirme yapılması (örneğin, yalnızca uygulama kullanılırken izin verilmesi),
- Mobil uygulamalara giriş yapılması adına sosyal medya hesaplarının kullanımından kaçınılması,
- Mobil uygulamalara giriş yapılması sırasında kullanılacak parolaların, güçlü kombinasyonlar ile oluşturulması, hesaplarda mümkün olduğu ölçüde farklı parola kullanılması ve çok faktörlü doğrulamanın etkinleştirilmesi,
- Mobil uygulamaların güncel tutulması ve güncelleme sonrasında gizlilik ayarlarının kontrolü,
- Kullanılmayan uygulamaların cihazda bulundurulmaması.



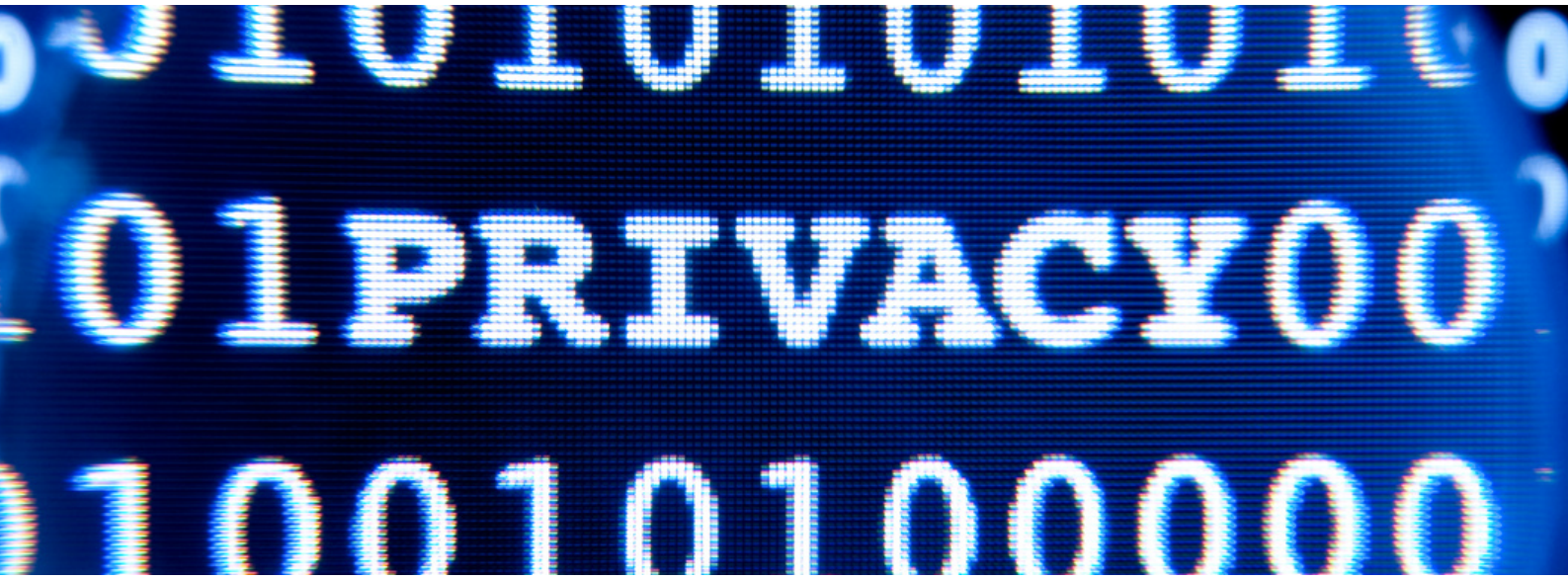
D) Kişisel Veri İşleyen Taraflara Yönelik Tavsiyeler

Rehber, ayrıca; mobil uygulamaların geliştirilmesi, kullanıma sunulması ve ilgili kişilerce kullanılması süreçlerinde yer alan aktörlerin veri sorumlusu ve veri işleyen sıfatlarının tespit edilerek bu kişilerce göz önünde bulundurulması gereken hususlara yer vermektedir. Bu hususlar kısaca şu şekildedir:

i. Genel ilkelere uyumluluk: Mobil uygulamalar kapsamında işlenen kişisel verilerin, KVKK'nın 4. maddesinde sayılan ilkelere uygun biçimde işlenmesi gerekmektedir.

- **Hukuka ve Dürüstlük Kurallarına Uygun Olma:** Uygulama geliştiricileri ve sağlayıcıları; kişisel veri işleme faaliyeti öncesinde, işleme bakımından hukuki sebebin ne olduğunu tespit etmeli, mobil uygulamalar aracılığıyla işlenen kişisel veriler bakımından dürüst ve şeffaf olmalı, ilgili kişilerin haklarını kullanmasına imkân sağlamalı ve buna elverişli tasarımlar sunmalıdır.

- **Doğru ve Gerektiğinde Güncel Olma:** Mobil uygulama kapsamında; ilgili kişilere, kişisel verilerini düzeltme imkânı ve buna elverişli tasarımlar sunulmalıdır.



- **Belirli, Açık ve Meşru Amaçlar İçin İşlenme ile İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma:** Mobil uygulama kapsamında; belirlenen amaca ulaşılabilmesi bakımından gerekli olan kişisel veri kategorileri tespit edilmeli ve bu doğrultuda mümkün olan en az çeşit ve sayıda kişisel verinin toplanması hedeflenmelidir.

- **İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme:** Mobil uygulamalar kapsamında işlenen kişisel veriler bakımından; yasal yükümlülükler veya iş ihtiyaçlarına dayanan saklama ve imha süreleri belirlenmeli ve gerekli olan süreden daha uzun süre saklanmamalıdır.

ii. Şeffaflığın Sağlanması: Mobil uygulamalar kapsamında, KVKK'nın 10. maddesine ve "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"e uygun şekilde davranılması hususu vurgulanmıştır.

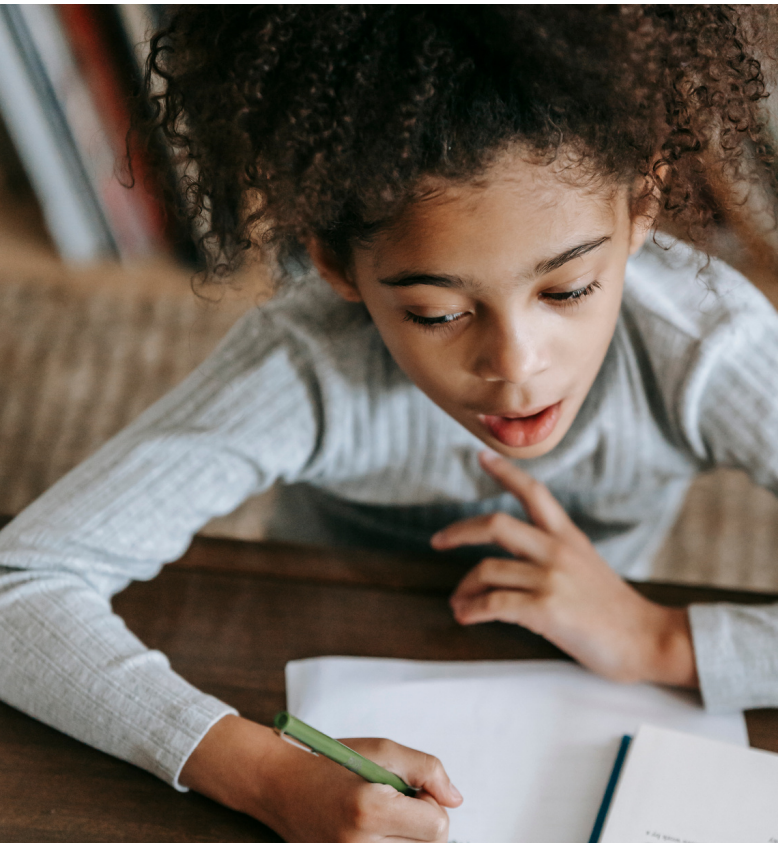
Buna ilave olarak, aydınlatma metni ile gizlilik politikası gibi metinlerin, ilgili kişilerce kolaylıkla ulaşılabilecek şekilde konumlandırılması, uygulama kapsamında gerçekleştirilen güncellemeler ile kişisel verileri ilgilendiren değişiklikler bakımından kullanıcıların bilgilendirilmesi, özellikle yurt dışında yerleşik sağlayıcılar bakımından Veri Sorumluları Sicili'ne (VERBİS) kayıt ve bildirim yükümlülüklerinin yerine getirilmesi gibi konulara yer verilmiştir.

Mobil Uygulamalarda Çocukların Kişisel Verilerinin İşlenmesi:
Ayrıca, çocuklara yönelik veya çocuklar tarafından yaygın şekilde kullanılan mobil uygulamalar kapsamında;

- Kullanıcı yaşını doğrulayacak sistemler kurulması,
- İşleme faaliyetlerinin ayrı bir politika ve prosedür çerçevesinde gerçekleştirilmesi

önerilmiştir.

iii. Kişisel Verilerin İşlenme Şartlarının Belirlenmesi: Rehber, mobil uygulamalar kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri bakımından, işleme şartlarının tespit edilmesinin önemini vurgulamış ve bu hususun, şeffaflığın sağlanması bakımından ön koşul teşkil ettiğinin altını çizmiştir.



Aynı zamanda Rehber, mobil uygulamanın esas işlevi bakımından gerekli olmayan kişisel verilere ilişkin olarak açık rıza alınması ve bu anlamda açık rızanın, geçerlilik şartlarını sağlayacak şekilde alınmasının önemine değinmiştir.

iv. Veri Güvenliğinin Sağlanması: Rehberde, mobil uygulamalar kapsamında veri güvenliğinin sağlanmasına ilişkin olarak da çeşitli öneriler sunulmuştur.

- Mobil uygulamaların; tasarımdan itibaren mahremiyet (privacy by design) ve başlangıçtan itibaren mahremiyet (privacy by default) ilkelerine uygun tasarlanması, kişisel veriler bakımından en üst düzey korumayı sağlayacak biçimde kullanıma sunulması,

- Yetkisiz erişimin önlenmesi adına cihazlarda kimlik doğrulama yöntemlerinin kullanılması,

- Çok faktörlü kimlik doğrulama yöntemlerinin kullanılmasının teşvik edilmesi,

- Mobil uygulamalara erişim sırasında kullanılacak parolaların, güçlü kombinasyonlar ile oluşturulması, bu parolaların belirli aralıklarla değiştirilmesinin sağlanması,

- Parolalar, yeterli güvenlik önlemleri alınmak kaydıyla saklanması, ayrıca "özet/karma" fonksiyonlarından geçirilerek muhafaza edilmesi,

- Düzenli şekilde yama yönetimi ve yazılım güncellemesi gerçekleştirilmesi,

- Uygulamanın yayımından önce, yazılım testlerinin uygun şekilde gerçekleştirilmesi ve uygulamanın bu testleri eksiksiz ve başarı ile geçtiğinin güvence altına alınması,

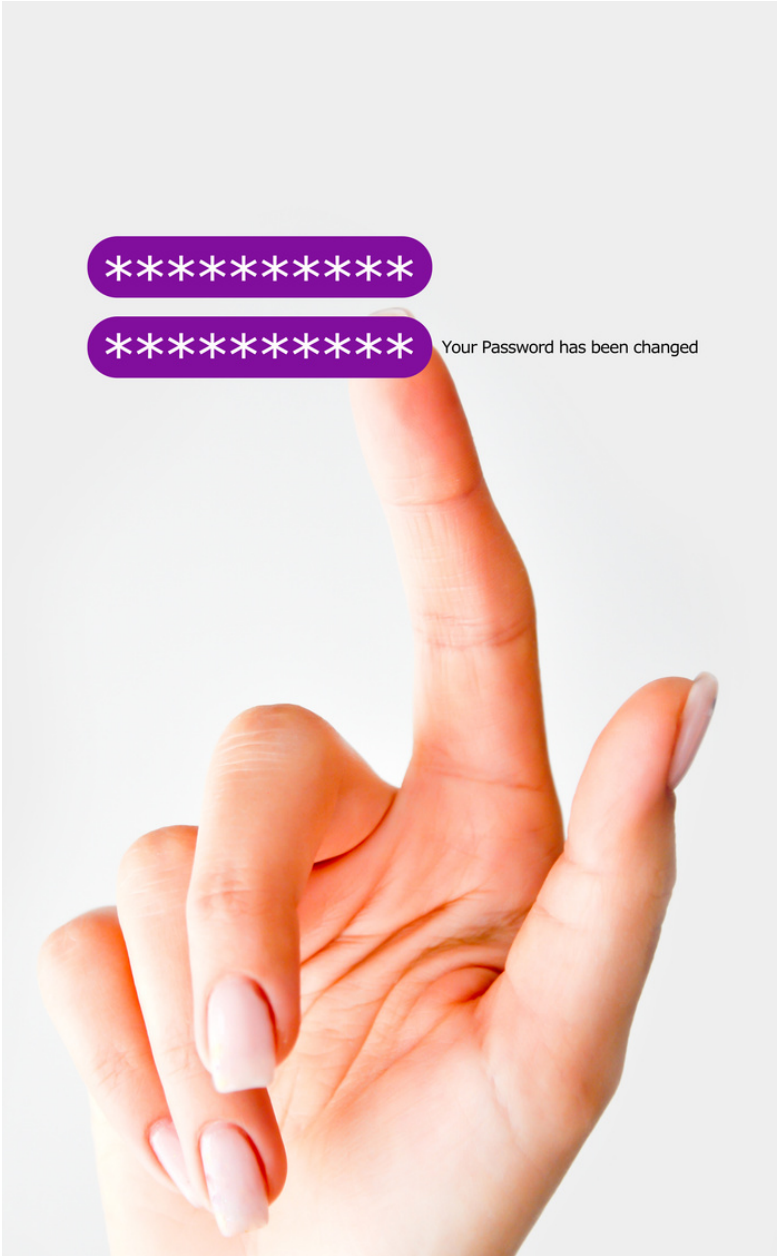
- Uygulama güvenliğinin, tasarım aşamasında başladığı göz önünde bulundurularak güvenli yazılım geliştirme stratejileri yürütülmesi,

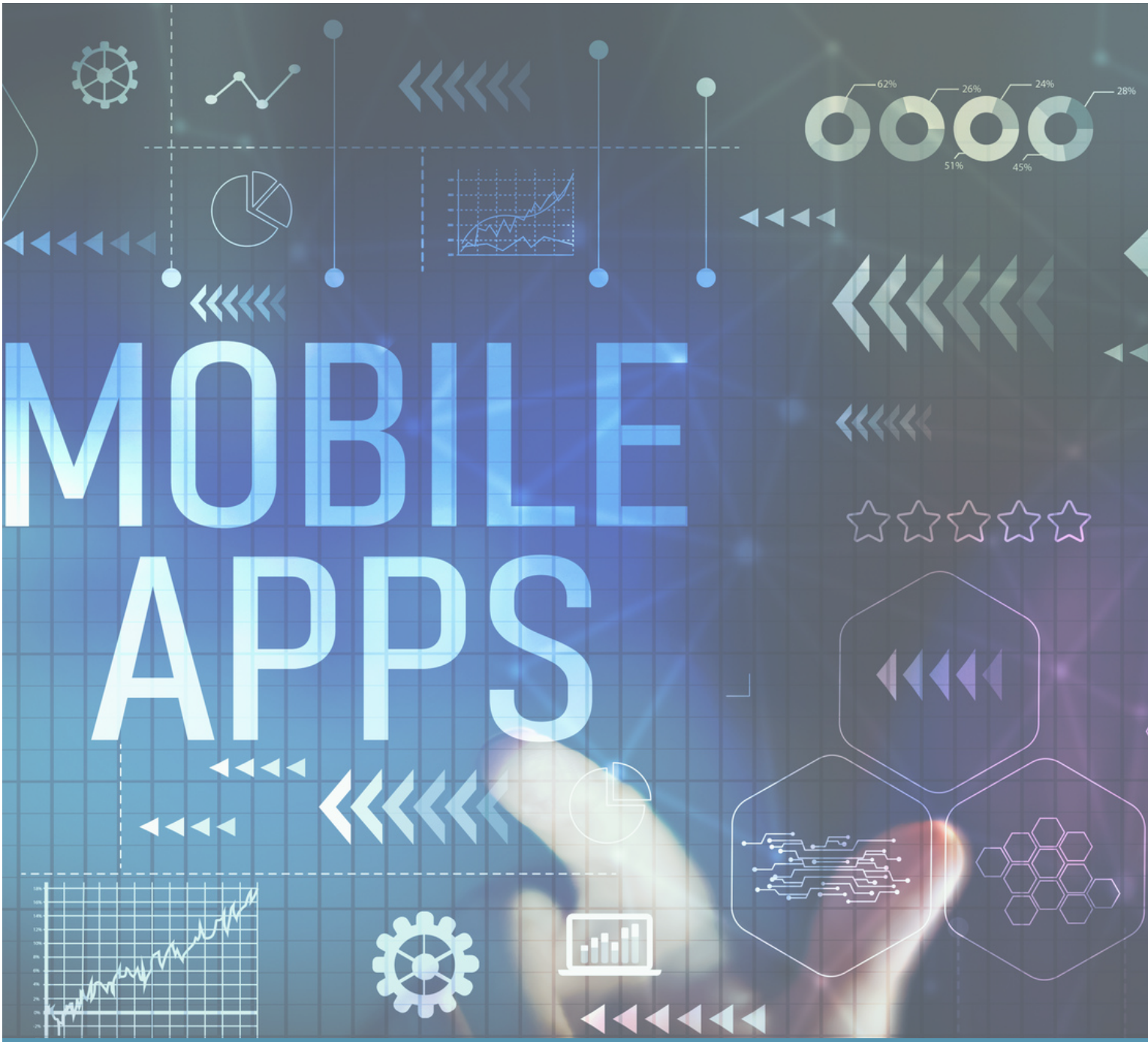
- Kullanıcıların, hesaplarına giriş sağlarken başarısız giriş sayısının sınırlandırılması, kullanıcı giriş sayfalarında CAPTCHA, dört işlem ve benzeri yöntemlerin kullanılması,

- Uygulamanın yayımından önce, hedeflenen işletim sistemlerinin veri koruma ve güvenlik özelliklerinin dikkate alınması, risk değerlendirmesi gerçekleştirilmesi,

- Mobil uygulamalarda kişisel verilerin depolanması ve aktarımı sırasında veri güvenliğinin sağlanması kapsamında, ağ iletişiminde uygun şekilde yapılandırılmış yeterli bir şifreleme katmanı ve ilgili şifreleme anahtarlarının güvenli yönetimi aracılığıyla koruma için şifreleme kullanılması.

Rehberin tamamına buradan ulaşabilirsiniz.





MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

P: +90 212 264 50 00
info@mclegal.com.tr | mclegal.com.tr
Nisbetiye Mah. Nisbetiye Cad. No:32/9
Beşiktaş / İSTANBUL