KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

MOBİL UYGULAMALARDA MAHREMİYETİN KORUNMASINA YÖNELİK TAVSİYELER

KVKK YAYINLARI NO: 46

MOBİL UYGULAMALARDA MAHREMİYETİN KORUNMASINA YÖNELİK TAVSİYELER

ARALIK 2023

KİŞİSEL VERİLERİ KORUMA KURUMU
Nasuh Akar Mah. 1407. Sokak No:4 06520 Balgat-Çankaya/Ankara
Tel: 0 (312) 216 50 00 // Faks: 0 (312) 216 50 52
Web: www.kvkk.gov.tr

TANIMLAR

Dokümanda yer alan;

İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,

Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Mobil Uygulama Geliştiricisi: Mobil cihazlar üzerinde kullanılmak üzere çeşitli yazılım ve uygulamaları tasarlayan ve geliştiren gerçek veya tüzel kişiyi,

Mobil Uygulama Sağlayıcısı: Kullanıcılara veya kuruluşlara internet üzerinden mobil uygulamalara ve ilgili mobil hizmetlere erişim imkânı sunan gerçek veya tüzel kişiyi,

Sicil: Veri Sorumluları Sicilini,

Uygulama Mağazası: Kullanıcıların çeşitli mobil uygulamaları ücretli ya da ücretsiz olarak indirebildikleri çevrim içi uygulama dağıtım platformunu,

VERBİS: Veri Sorumluları Sicil Bilgi Sistemini,

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi

ifade eder.

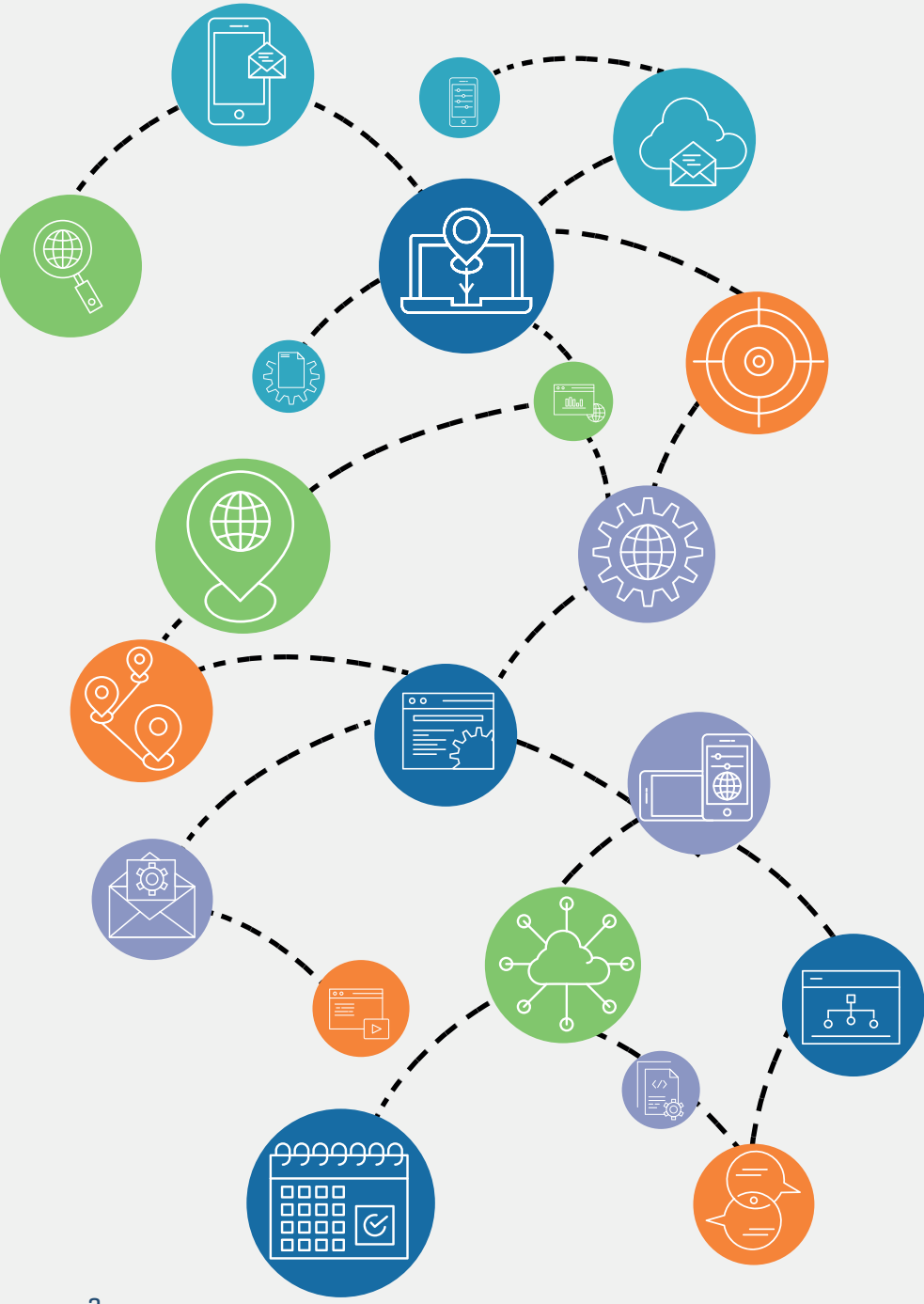
AMAÇ VE KAPSAM

Hayatın birçok alanında kolaylık ve erişilebilirlik sağlayan mobil cihazlar modern yaşamın ayrılmaz bir parçası hâline gelmiştir. Taşınabilir olma özelliği ile ön plana çıkan ve kablosuz iletişim teknolojileri aracılığıyla internete veya diğer ağlara bağlanabilen elektronik aygıtlar olan mobil cihazlar; akıllı telefon, tablet, dizüstü bilgisayar ve giyilebilir teknoloji gibi ürün kategorilerini temsil etmektedir. Bu dokümanda ise akıllı telefonlar ve tabletlerde kullanılan mobil uygulamalar aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetlerine odaklanılmıştır.

Günümüzde gelinen noktada dijital altyapının hızlı bir şekilde büyümesi ve mobil cihazların genel kullanımının artmasıyla birlikte mobil uygulamalar da günlük yaşantımızın vazgeçilmez unsurları arasına girmiştir. Mobil cihazlarda çalışacak şekilde tasarlanmış yazılım programları olarak ifade edilebilecek mobil uygulamalar, hava durumunu kontrol etmekten gerçek zamanlı haber güncellemelerini almaya, bankacılık işlemleri gerçekleştirmekten sağlık durumunun takibine ve sosyal medya kullanımından çevrim içi alışveriş yapmaya kadar akla gelebilecek pek çok konuda hizmet sunmakta ve günlük hayatın birçok alanında bireylere çeşitli kolaylıklar sağlamaktadır.

İçinde bulunduğumuz çağın teknolojik dinamiklerinde, bireyler mobil cihazlarını her daim yanlarında bulundurmakta ve çeşitli kişisel verilerini uzun süreler boyunca cihazlarında muhafaza etme eğilimi göstermektedirler. Günümüzde mobil cihazların mikrofon, kamera, ivmeölçer, GPS, Wi-Fi ve Bluetooth gibi birçok sensöre sahip olduğu, işlemcileri ve yerel depolama kabiliyeti gibi teknik özelliklerinde gelişme sağlandığı, mobil uygulama geliştiricileri tarafından bulut hizmetlerinin yaygın şekilde kullanıldığı ve mobil cihazların kullanıcının neredeyse tüm yaşamının ayrılmaz bir parçası hâline geldiği dikkate alındığında, mobil uygulamalarda bireylerin kişisel verilerinin korunmasının kritik bir öneme sahip olduğu yadsınamaz.

Bilindiği üzere, kişisel verilerin korunması bireyin mahremiyetinin korunmasına hizmet etmektedir. Dolayısıyla kişisel verilerin korunması hususunu teknolojik gelişmelerin bir parçası hâline getirmek, bireyin mahremiyetinin korunması bakımından elzemdir. Bu dokümanda, mobil uygulamalarda mahremiyetin korunmasına yönelik mevcut ve potansiyel risklerin ele alınması ile akıllı telefonlar ve tabletlerde kullanılan mobil uygulamalar aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetleri bakımından ilgili kişi ve veri sorumlusu niteliğini haiz aktörlere yönelik genel nitelikli tavsiyelerde bulunulması amaçlanmaktadır.



A. MOBİL UYGULAMALARDA İŞLENEN KİŞİSEL VERİLER

Bir ülkede yürürlükte olan veri koruma mevzuatının uygulanmasına ilişkin ilk koşul, ilgili faaliyet kapsamında bireylerin "kişisel veri"lerinin işlenmiş olmasıdır.

Ülkemizde yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 3'üncü maddesinin (1) numaralı fıkrasının (d) bendi uyarınca kişisel veri, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*yi ifade etmekte olup "kişisel verilerin işlenmesi" kavramı ise anılan maddenin (e) bendinde, *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi,*

değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" şeklinde tanımlanmaktadır.

Mobil uygulamalarda, kullanıcı deneyimini zenginleştirmek, işlevsellik sağlamak, sunulan hizmeti iyileştirmek ve pazarlama stratejileri oluşturmak gibi amaçlar doğrultusunda hem kişisel veriler hem de kişisel veri niteliğini haiz olmayan çeşitli veriler işlenebilmektedir. Bu kapsamda, uygulamanın işlevselliğine, tasarımına ve kullanıcının verdiği izinlere göre değişkenlik gösterecek şekilde, mobil uygulamalar tarafından işlenen kişisel verilerden bazıları aşağıdaki şekilde örnek gösterilebilir:


Kimlik bilgileri (ad ve soyadı, 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[1], MAC[2] adresi, IMEI[3] ve IMSI[4] numarası, cihazda yüklü uygulama listesi aracılığıyla parmak izi çıkarılması[5,6] 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.

---

1 IP Adresi *(Internet Protocol Address)*, cihazların ağ üzerinde birbirleriyle veri alışverişi yapmalarını sağlayan bir protokol olarak tanımlanabilmektedir.

2 MAC Adresi *(Media Access Control)* / (Tekil Ağ Cihaz Numarası),bir ağ cihazını benzersiz olarak tanımlayan fiziksel adres şeklinde tanımlanabilmektedir.

3 IMEI Numarası *(International Mobile Equipment Identity)* / (Uluslararası Mobil Cihaz Kodu): Mobil cihazlara ait uluslararası elektronik kimlik bilgisini gösteren numara. *(Elektronik Kimlik Bilgisini Haiz Cihazların Kayıt Altına Alınmasına Dair Yönetmelik, Madde 4 (1)(g).*

4 IMSI Numarası *(International Mobile Subscriber Identity)* / (Uluslararası Mobil Abone Tanımlayıcısı): GSM mobil sistemlerinde SIM kart için tanımlayıcı sayı dizisi. *(Elektronik Kimlik Bilgisini Haiz Cihazların Kayıt Altına Alınmasına Dair Yönetmelik, Madde 4 (1)(o).*

5 Achara, J.P./Acs, G./Castelluccia, C.: *On the Unicity of Smartphone Applications*, Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society (2015), (https://api.semanticscholar.org/CorpusID:15723203), s. 2.

6 Pham, A.: *Privacy-Enhancing Technologies for Mobile Applications and Services* (2019), (https://api.semanticscholar.org/CorpusID:86537250).

Bu kapsamda örneğin, uygulamaların kişinin telefon rehberine veya diğer uygulamalardaki arkadaş listelerine erişimi, bireyin kendisi ve rehberindeki ya da kullandığı uygulamalardaki arkadaş listelerindeki kişilerin sosyal bağlantıları hakkında bilgi sunabilmektedir. Konum bilgisi ise kullanıcıların etkinlik kalıplarını ve alışkanlıklarını ortaya çıkarabilmekte ve diğer yandan kullanıcıyı tanımlama amacıyla başvurulan çevrim içi tanımlayıcı değerleri ile kullanıcı hakkında detaylı profiller oluşturulabilmektedir.

Kişisel verilerin daha sıkı tedbirlerle korunmasını gerektiren bir veri kategorisi olarak "özel nitelikli (hassas) kişisel veriler" ise başkaları tarafından öğrenildikleri takdirde bireyin mağdur olmasına ya da ayrımcılığa maruz kalmasına neden olabilecek nitelikteki veriler olarak kabul edildiğinden, bu tür verilerin diğer kişisel verilere göre çok daha sıkı şekilde korunması gerekmektedir.

Bu nedenle Kanun'da bu verilere özel bir önem atfedilmekte ve hangi kişisel verilerin özel nitelikli kişisel veri sıfatını haiz olduğu ve özel nitelikli kişisel verilerin işlenme şartları Kanun'da ayrıca düzenlenmektedir. Bu çerçevede Kanun'un 6'ncı maddesinin (1) numaralı fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri, sınırlı sayma yoluyla, özel nitelikli kişisel veriler olarak sayılmaktadır.

Bu kapsamda örneğin, ses tanıma uygulamalarında ses izi biyometrisi kullanılması suretiyle kişi hakkında biyometrik veri toplanabilmektedir[7]. Sağlık uygulamalarında ise doğrudan sağlık verisi toplanmakla birlikte bazı durumlarda fotoğraflar, mesajlar ve kullanıcı girişleri gibi ögeler de özel nitelikli kişisel veri içerebilmektedir. Ayrıca görseller, bazı durumlarda kişilerin etnik kökenini veya ırkını; mesajlar ise kişilerin inancını, siyasi düşüncesini veya sağlık durumunu ortaya çıkarabilmektedir.

7 Office of the Privacy Commissioner of Canada/Office of the Information and Privacy Commissioner of Alberta/Office of the Information&Privacy Commissioner for British Columbia: Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps (2012), https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/ ,s.3.

B. MOBİL UYGULAMALARDA VERİ SORUMLUSU-VERİ İŞLEYEN[8]

Mobil uygulamalar söz konusu olduğunda, kişisel verilerin işlenmesi ve korunması süreçlerinde; uygulama sağlayıcısı, uygulama geliştiricisi, reklam ağı, uygulama mağazası kuruluşu, işletim sistemi sağlayıcısı, kütüphane sağlayıcısı ve cihaz üreticisi başta olmak üzere birçok aktöre sorumluluk düşmektedir.

Genellikle uygulama sağlayıcısı, kullanıcıların kişisel verilerini kendi amaçları doğrultusunda kullandığı ölçüde, kişisel verilerin işlenmesinde Kanun kapsamında veri sorumlusu olarak kabul edilecektir. Ancak mobil uygulamalarda toplanan kişisel veriler bakımından birden fazla veri sorumlusu ortaya çıkması ihtimali de bulunmaktadır. Bu kapsamda mobil uygulamanın, üçüncü taraf bir hizmeti uygulamasına entegre ettiği durumda (örneğin, dolandırıcılığın önlenmesi amacıyla iki faktörlü kimlik doğrulama yapmak üzere üçüncü taraf hizmet sağlayıcının mobil uygulamaya dahil olması ya da mobil uygulamada yer alan reklam ağları) birden fazla veri sorumlusu ortaya çıkabilecektir. Cihazda

8 Bu bölümde yer verilen senaryolar örnek niteliğindedir. Kişisel Verileri Koruma Kurulu, kendisine intikal ettirilen şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen yapacağı incelemede, mobil uygulamalar aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetleri bakımından somut olayın özelliklerini göz önünde bulundurarak değerlendirmesini yapacaktır.

yüklü uygulamalar kullanıldığında, işletim sistemi sağlayıcısı verileri bir araya getirebilir[9] ve kullanıcının cihazındaki uygulamalardan topladığı kişisel verileri kendi amaçları doğrultusunda kullanabilir. Böyle bir durumda, işletim sistemi sağlayıcısının veri sorumlusu olması ihtimali gündeme gelecektir.

Uygulama sağlayıcısı ve geliştiricisinin ayrı kuruluşlar olduğu bir durumda, uygulama sağlayıcısı ile geliştiricisi arasındaki sözleşmeye göre, uygulama geliştiricisinin kişisel veri işlemede yalnızca teknik bir rol üstlenmesi ve kendi amaçları doğrultusunda kişisel veri işlememesinin güvence altına alınması hâlinde, uygulama geliştiricisi veri işleyen olarak nitelendirilebilecektir. Diğer yandan, mobil uygulamalardan toplanan kişisel veriler genellikle bulutta depolanmakta olup uygulama geliştiricisi tarafından kullanılan bulut hizmetleri söz konusu olduğunda da veri işleyen sıfatının ortaya çıkması ihtimali gündeme gelebilecektir.

9 The European Union Agency for Network and Information Security (ENISA): *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (2017), https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications ,s.16.

C. BİREYLERE YÖNELİK TAVSİYELER

1. Mobil Uygulama Yüklenmeden Önce Dikkat Edilmesi Gerekenler

Uygulamanın güvenilir bir kaynaktan geldiğinden emin olunmalı ve uygulama, güvenilir olduğu değerlendirilen platformlar (örneğin, uygulama mağazaları) üzerinden cihaza indirilmelidir. Zira cihazın üreticisi veya işletim sistemi tarafından sağlanan resmi uygulama mağazaları veya mobil uygulama sağlayıcısının resmi internet sitesi gibi daha güvenilir kaynakların kullanılması, tehlikeli olabilecek uygulamaların cihaza yüklenmesi riskini azaltabilecektir.

Bir uygulama yüklenmeden önce uygulamanın geliştiricisi hakkında bilgi edinilmeli ve uygulama adının doğruluğundan emin olunmalıdır. Bu çerçevede, resmi olarak yayımlanan uygulamaları taklit eden ve kaynağı bilinmeyen uygulamalardan uzak durulmalıdır.

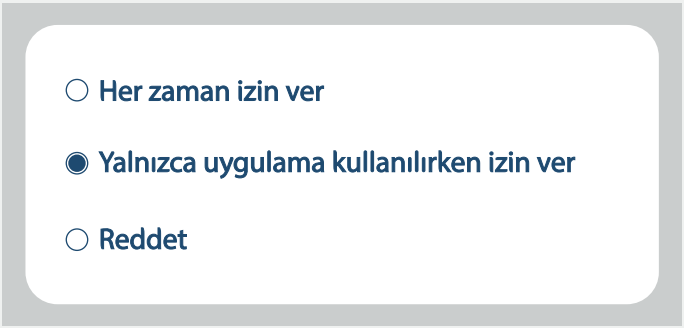
Uygulamanın işlevselliği ile güvenilirliği hakkında fikir edinmek için uygulamaya yönelik kullanıcı yorumlarının ve uygulamanın kullanıcılardan aldığı puanın kontrol edilmesi faydalı olacaktır. Bununla birlikte yüksek uygulama puanının ve olumlu yorumların bir uygulamayı mutlak surette güvenilir hâle getirmediği de unutulmamalıdır.

Uygulama yüklenmeden önce hangi verilere erişim izni istendiği kontrol edilmeli ve uygulamanın gizlilik politikası gözden geçirilmelidir. Uygulamanın sunduğu hizmet ile herhangi bir ilişkisi bulunmayan kişisel veri taleplerine karşı dikkatli olunmalıdır. Hizmetin sunulması için gerekli olandan daha fazla kişisel veri talep edilmesi durumunda, bu uygulamaya gerçekten ihtiyaç duyulup duyulmadığı değerlendirilmeli ve gerekiyorsa alternatif uygulamalar araştırılmalıdır.

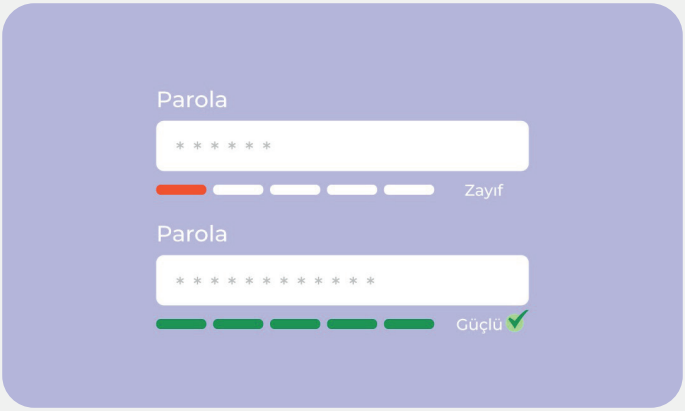
2. Mobil Uygulamanın Kullanılması Sürecinde Dikkat Edilmesi Gerekenler

- Uygulamanın kullanımı sırasında talep edilen izinler konusunda da dikkatli olunmalıdır. Örneğin; bir navigasyon uygulamasında kullanıcıya doğru yön ve konum bilgilerinin sağlanabilmesi için kullanıcının "anlık konumunu" kullanma izni istenmesi veya bir fotoğraf düzenleme uygulamasında, fotoğraflara erişim izni istenmesi olağan bir durum olarak kabul edilmektedir. Ancak bazı uygulamalarda, uygulamanın belirli bir işlevselliği için ihtiyaç duyulmayan verilere erişim için ilave izinler de istenebilmektedir. Kullanım sırasında uygulama tarafından talep edilen izinler konusunda, mahremiyetin korunmasına yönelik endişe duyulması hâlinde erişim isteklerinin reddedilmesi ve alternatif bir uygulama araştırılması hususunun değerlendirilmesi faydalı olacaktır.

- Konum, ses ve görüntü verileri elde eden mobil cihaz araçlarına sürekli erişilmesine ilişkin izinlerin, söz konusu verilerin kullanım amaçları dikkate alınarak değerlendirilmesi uygun olacaktır.

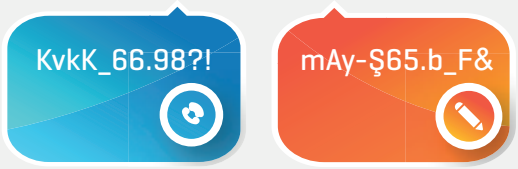


- Uygulamalara giriş yapmak için sosyal medya hesaplarının kullanılmasından kaçınılmalıdır. Zira bir uygulamada kullanıcının sosyal ağ hesabına ilişkin bilgiler ile oturum açılması, kimi durumlarda uygulamanın ilgili sosyal ağ hesabından bilgi toplamasına olanak tanıyabilmekte ve hesapları tehditlere karşı daha savunmasız hâle getirebilmektedir.



- Uygulamalara giriş yapmak için kullanılacak parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay şekilde tahmin edilebilecek rakam ya da harf dizileri yerine büyük-küçük harf, rakam ve sembolleri içerecek şekilde güçlü kombinasyonlar tercih edilmelidir. Mümkün olduğu durumlarda her hesap için farklı parola oluşturulmalı ve çok faktörlü doğrulama etkin hâle getirilmelidir.

GÜÇLÜ PAROLA ÖRNEKLERİ



- Güncel olmayan yazılımlara sahip uygulamalar, saldırıya uğrama riskiyle daha fazla karşı karşıya kalabileceğinden uygulamalar güncel tutulmalıdır. Ayarların ve yapılandırmaların değişmediğinden emin olmak için güncelleme yapıldıktan sonra gizlilik ayarları kontrol edilmelidir.

- İhtiyaç duyulmayan ve kullanılmayan uygulamalar mobil cihazlarda bulundurulmamalıdır.

Ç. KİŞİSEL VERİ İŞLEYEN TARAFLARA YÖNELİK TAVSİYELER

Mobil uygulamaların geliştirilmesi, kullanıma sunulması ve ilgili kişiler tarafından kullanılması süreçlerinde farklı paydaşların veri sorumlusu veya veri işleyen olma statüleri kişisel veri işleme faaliyetine başlanmadan önce belirlenmelidir. Bu kapsamda, her bir paydaşın veri koruma mevzuatı bağlamındaki sorumluluğu ve paydaşlar arasındaki hukuki ilişki netleştirilerek Kanun ve ikincil mevzuata uyum sağlanmalıdır.

1. Genel İlkelere Uyumluluk

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Genel İlkeler" başlıklı 4'üncü maddesinde kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde;

a) Hukuka ve dürüstlük kurallarına uygun olma,
b) Doğru ve gerektiğinde güncel olma,
c) Belirli, açık ve meşru amaçlar için işlenme,
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenlenmektedir. Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hâl ve şartta Kanun'un 4'üncü maddesinde sayılan ilkelere uyulması hukuki bir gereklilik olup mobil uygulamalar vasıtasıyla işlenen kişisel veriler de Kanun'un bahse konu maddesinde düzenlenen ilkelere uygun şekilde işlenmelidir.

a) Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi

Hukuka ve dürüstlük kuralına uygun olma ilkesi, kişisel verilerin işlenmesinde kanunlarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade etmektedir. Dürüstlük kuralına uygun olma ilkesi uyarınca veri sorumlusu, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almalıdır. Diğer bir ifade ile, ilgili kişinin beklemediği ve beklemesinin de gerekmediği sonuçların ortaya çıkmasını önleyici şekilde hareket etmesi gerekmektedir. Ayrıca ilke uyarınca, ilgili kişi için söz konusu veri işleme faaliyetinin şeffaf olmasının sağlanması ve bilgilendirme yükümlülüğüne uygun hareket edilmesi gerekmektedir.

Bu kapsamda uygulama geliştiricileri ile sağlayıcılarının kişisel veri işlemeye başlamadan önce işlemenin bir hukuki sebebinin olup olmadığını sorgulamaları, mobil uygulamalarda işlenen kişisel veriler konusunda dürüst ve şeffaf olmaları, bireylerin haklarını kullanabilmelerine imkân sağlamaları ve bu hakların kullanımını destekleyen süreç ve tasarımları uygulamaya koymaları beklenmektedir.

Mobil ortamda karşılaşılan en önemli sorunlardan birisi, izin mimarilerinin uygulamaya ve uygulamaya entegre üçüncü taraflara ayrı ayrı izin verme imkânı sağlamamasıdır[10]. Bazen bir uygulama, yalnızca üçüncü bir taraf belirli bir veri türüne erişmek istediği veya bu veriye ihtiyaç duyduğu için cihazdaki bu veri türüne erişim talebinde bulunabilir. Uygulamada faydalanılan üçüncü taraf işlemeleri hakkında şeffaf olunması ve uygulamaya entegre edilen üçüncü taraf hizmet aracılığıyla kişisel veri işlenmesinde hukuki bir sebep bulunmadığı takdirde bu hizmetin uygulamada kullanılmaması önem taşımaktadır.

10 ENISA, a.g.e., s.20.

Örnek-1

Günümüzde mobil cihazlar, ses kontrol asistanları tarafından desteklenerek sesli komut ile çalışabilmekte ve bu asistanlar aktive edildiğinde tüm sözlü iletişime erişebilmektedirler. Bu kapsamda, işlenen kişisel veriler hakkında şeffaflık sağlanması gerekmektedir. Diğer taraftan, mobil uygulama ilk kullanıma başlandığında, bu özelliğin cihazda kural olarak açık şekilde gelmesi, hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil edebilecektir. Öte yandan örneğin, cep telefonu masanın üzerinde dururken yahut kişinin cebinde veya çantasında iken mikrofona erişim sağlanması yerine, kullanıcı cihazı aktif bir şekilde kullanırken mikrofona erişim sağlanması gibi önlemlerle, kişisel verilerin işlenmesinde kullanıcının makul beklentisi karşılanabilecektir.

Örnek-2

Adım sayarak ve uyku düzeni ile beslenme alışkanlıklarını izleyerek bireylerin fiziksel aktivite seviyelerini takip eden bir mobil uygulamanın, elde ettiği bu verilere ilişkin istatistiki bilgiler oluşturmanın yanında, kullanıcılara egzersiz yapmalarını hatırlatmak suretiyle de söz konusu verileri işlemesinin mobil uygulamanın kullanım amacıyla uyumlu olduğu söylenebilecektir. Aynı doğrultuda, kullanıcılar da bu durumu memnuniyetle karşılayabilirler. Ancak, bahse konu mobil uygulama sağlayıcısının sağlık sigortası hizmeti sunması ve mobil uygulama üzerinden topladığı kişisel verilerden sigorta primi hesaplamada yararlanması, kullanıcının makul beklentisinin aşılması nedeniyle, dürüstlük kuralına aykırılık teşkil edebilecektir[11].

11 World Intellectual Property Organization (WIPO): *A Guide to Data Protection in Mobile Applications* (2021), [https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf], s. 24.

b) Doğru ve Gerektiğinde Güncel Olma İlkesi

Kişisel verilerin doğruluğunun ve güncelliğinin önemini vurgulayan "doğru ve gerektiğinde güncel olma" ilkesi ile 6698 sayılı Kanun'da öngörülen ilgili kişinin verilerinin düzeltilmesini talep etme hakkı uyumludur. Kişisel verilerin doğru ve güncel bir şekilde tutulması, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gereklidir. Kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında aktif özen yükümlülüğü; veri sorumlusu eğer bu verilere dayalı olarak ilgili kişiyle alakalı bir sonuç ortaya koyuyor ise geçerlidir. Bunun dışında veri sorumlusu her zaman ilgili kişinin bilgilerinin doğru ve güncel olmasını temin edecek kanalları açık tutmalıdır.

Söz konusu ilke mobil uygulamalar bağlamında değerlendirildiğinde, kullanıcılara kişisel verilerini düzeltme imkânı tanınmalı ve uygulamanın tasarımı sürecinde bu hususun göz önünde bulundurulması suretiyle uygulama içerisinde uygun yöntemlerle bu imkânın kullanılması sağlanmalıdır. Diğer yandan, güncelliğini yitirmiş kişisel verilerin kimlik hırsızlığı riski ortaya çıkarabileceği unutulmamalıdır[12].

12 ENISA, a.g.e, s.22.

Örnek-3

Bir mobil uygulamaya üye olunması esnasında kullanıcı tarafından e-posta ve telefon numarası bilgilerinin girildiği ancak söz konusu mobil uygulamada bu bilgiler için herhangi bir doğrulama yapılmadığı ve kullanıcılara uygulama içinden bu bilgileri güncelleme fırsatı sunulmadığı bir durumda; kullanıcı, üyelik esnasında e-posta adresini sehven hatalı girmiş ve mobil uygulama üzerinden gerçekleştirdiği alışverişe ilişkin sipariş bilgileri bu e-posta adresine gönderilmişse kişisel verilerin üçüncü bir kişiye ifşa olması ihtimali gündeme gelebilecektir. Dolayısıyla bu uygulama, eğer kullanıcının e-posta adresini doğrulamış olsaydı bu tür bir ifşa ortaya çıkmayacak ve söz konusu ilkeye uygun hareket edilmiş olacaktı.

Benzer şekilde, kullanıcının belli bir süre sonra telefon numarasını değiştirmesi ve mobil uygulamasının parolasını unuttuğu için mobil uygulama aracılığıyla parola sıfırlama talebinde bulunması durumunda, kullanıcının parola sıfırlaması esnasında daha önce girmiş olduğu ve artık kullanmadığı telefon numarasına kod gönderilmesi durumunda, kodun üçüncü bir kişiye mesaj olarak iletilmesi riski ortaya çıkabilecektir. Eğer kullanıcıya uygulama içinde telefon numarasını kontrol etme ve güncelleme fırsatı sunulmuş olsaydı, kullanıcı da güncel olmayan telefon numarasını kontrol ederek değiştirme fırsatı bulabilecek ve söz konusu ilkenin gereği yerine getirilmiş olacaktı.

c) Belirli, Açık ve Meşru Amaçlar İçin İşlenme ile İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkeleri

Kanun'da düzenlenen ilkelerden bir diğeri olan, kişisel verilerin "belirli, açık ve meşru amaçlar için işlenme" ilkesi ise, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve bu faaliyetin gerçekleştirilme amacının belirliliği sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.

Bir diğer önemli ilke olan *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkesine göre ise, işlenen veriler belirlenen amaçların gerçekleştirilebilmesine elverişli olmalıdır. Amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi ve amaç için gerekli olmayan veri işlemeden kaçınılmasıdır. Ölçülülük ilkesi ise, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması anlamına gelmektedir. Diğer bir ifadeyle, veri işlemenin amacı gerçekleştirecek ölçüde olmasını ifade etmektedir.

Mobil uygulamalar aracılığıyla işlenen kişisel veriler açısından da işleme faaliyetinin amacının ortaya konulmasının ardından, söz konusu amacı gerçekleştirebilmek için hangi kişisel veri kategorilerine ihtiyaç duyulduğu belirlenmelidir. Bu belirleme yapılırken, mümkün olan en az çeşit ve sayıda kişisel veri toplanması hedeflenerek, kişisel verilerin işlenmesi bağlamında bireylerin temel hak ve özgürlüklerinin en üst düzeyde korunmasını sağlayacak bir yaklaşım benimsenmelidir. Bu doğrultuda, eğer bir kişisel verinin uygulama aracılığıyla sunulan işlev veya faaliyetlerle nasıl ilişkili olduğu açıklanamıyorsa, bu veriler toplanmamalıdır.

Diğer taraftan mobil uygulama üzerinden gerçekleştirilen işlemenin amaçla bağlantılı, sınırlı ve ölçülü olması, kullanıcılar bakımından öngörülebilirliğin sağlanması açısından da önem taşımaktadır. Bu çerçevede, mobil uygulama tarafından elde edilen kişisel veriler, bireylerin uygulamayı kullanım amacını aşar nitelikte işleme faaliyetlerine konu edilmemelidir.

Örnek-4

Bulaşıcı hastalıklarla mücadele amacıyla temas takibinde kullanılmak üzere hazırlanan bir mobil uygulama, yalnızca bireylerin yakınlık verisini (Bluetooth teknolojisi vasıtasıyla toplanan ve kişilerin birbirlerine hangi süre zarfında ne kadar yakın olduğunu gösterir bilgi) işlemek suretiyle kullanım amacını gerçekleştirebilecektir. Dolayısıyla, bu mobil uygulamanın kullanıcılarının tam konumunu ve hareketlerini izlemesi, kullanıcının bulaşıcı hastalığa sahip başka bir kullanıcıyla yakın temasta bulunduğunun tespit edilebilmesi amacı bakımından gereksiz olup bu nitelikteki bir işleme faaliyeti amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil edebilecektir[13].

Örnek-5

Mobil uygulamanın verdiği hizmet kapsamında gerçekleştirilecek işleme faaliyetlerinin, yalnızca mobil uygulamanın kullanıldığı cihazın yerel depolama alanında tutulacak kişisel veriler ile yürütülebilmesinin mümkün olduğu hâllerde, söz konusu kişisel verilerin mobil uygulama sağlayıcısının veri kayıt sistemlerine iletilmemesi "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine uygun olacaktır.

13 WIPO, a.g.e., s.25.

ç) İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi

"İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkesi uyarınca, kişisel verilerin, "amaçla sınırlılık ilkesi"nin de bir gereği olarak, işlendikleri amaç için gerekli olan süreye uygun şekilde muhafaza edilmeleri gerekmektedir. Bu konuda veri sorumlusu, gerekli teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin saklanmasında amaçla sınırlılık ilkesi uyarınca veri sorumlusu tarafından belirlenen saklama sürelerinin yanı sıra, veri sorumlusunun tabi olduğu ilgili mevzuat kapsamında da belirlenmiş saklama süreleri mevcuttur. Buna göre veri sorumluları, ilgili kişisel veriler için mevzuatta öngörülmüş bir süre varsa bu süreye uyacak; eğer böyle bir süre öngörülmemişse verileri ancak işlendikleri amaç için gerekli olan süre kadar saklayabileceklerdir. Bir verinin daha fazla saklanması için geçerli bir sebep bulunmaması hâlinde, o veri silinecek, yok edilecek veya anonim hâle getirilecektir. İleride tekrar kullanılabileceği düşünülerek ya da herhangi bir başka gerekçe ile kişisel verilerin muhafaza edilmesi yoluna gidilemeyecektir.

Mobil uygulamalar aracılığıyla işlenen kişisel veriler açısından da açıkça tanımlanmış iş ihtiyaçlarına veya yasal yükümlülüklere göre gerekçelendirilmiş saklama ve imha[14] süreleri belirlenmeli ve bu veriler gerekli olan süreden daha uzun süre saklanmamalıdır.

Bu çerçevede örneğin, bir mobil uygulama geliştiricisinin bulutta depoladığı kişisel veriler açısından saklama süresi, mobil uygulamanın kullanıldığı sektöre özel mevzuatta öngörülen azami bir saklama süresi varsa bu süre göz önünde bulundurularak belirlenmeli; eğer bu şekilde bir azami saklama süresi bulunmuyorsa bu verilerin işlendikleri amaçla bağlantılı bir saklama süresi belirlenmelidir. Ayrıca, saklama süresi dolan kişisel verilerin, bu verilerin imhasına ilişkin gerekli her türlü teknik ve idari tedbir alınarak imha edilmesinin beklendiği de belirtilmelidir.

14 28.10.2017 tarih ve 30224 sayılı Resmî Gazete'de yayımlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in 4'üncü maddesinin (1) numaralı fıkrasının (c) bendi uyarınca imha, *"kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi"* anlamına gelmektedir.

Örnek-6

Mobil uygulama üzerinden sunulacak hizmetin niteliğine göre sınıflandırılacak aktif ve aktif olmayan kullanıcıların kişisel verilerinin saklanma süreleri söz konusu statülere göre belirlenmelidir. Bu anlamda, elektronik posta hizmeti sunan bir mobil uygulamanın kullanıcısının, belirli bir süre boyunca uygulamaya giriş yapmaması durumunda statüsünün aktif olmayan kullanıcıya dönüştürülmesi ve aktif kullanıcılara kıyasla kişisel verilerinin saklanma süresinin daha kısa olması (yasal yükümlülükler hariç olmak üzere) bu hususta iyi uygulama örneği teşkil edebilecektir.

2. Şeffaflığın Sağlanması

Kanun'un "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesinde, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin, ilgili kişilere;

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
b) Kişisel verilerin hangi amaçla işleneceği,
c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
d) 11'inci maddede sayılan diğer hakları

konularında bilgi vermekle yükümlü olduğu düzenlenmiştir. Bu kapsamda, Kanun'un 10'uncu maddesinde yer alan aydınlatma yükümlülüğü, Kurul tarafından çıkartılan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" hükümlerine uygun olarak yerine getirilmelidir.

Diğer yandan, aydınlatma metni ve eğer ayrıca hazırlanmışsa gizlilik politikası, mevcut kullanıcıların ve uygulamayı indirmeyi düşünen potansiyel kullanıcıların kolaylıkla erişebilecekleri bir şekilde konumlandırılmalıdır.

Uygulamaya ilişkin güncellemeler konusunda kullanıcılar haberdar edilirken, kişisel verilerinin işlenmesini ilgilendiren değişiklikler konusunda da kullanıcılar bilgilendirilmelidir.

Kullanıcıların bir uygulamanın varsayılan gizlilik ayarlarından haberdar olmaları sağlanmalı ve gizliliklerini yönetmelerine yardımcı olacak anlaşılması kolay mekanizmalar, kullanıcı dostu bir arayüz ile sunulmalıdır.

Kullanıcıların bir uygulamanın kullanılması konusunda bilinçli kararlar verebilmelerini sağlamak üzere, Kanun'un 10'uncu maddesine uygun olarak bilgilendirme yapılmalıdır. Zira kişisel verilerin korunmasını isteme hakkının bir gereği olarak, bireylerin kişisel verileri üzerinde en üst düzeyde kontrole sahip olabilmeleri için, uygulamalar vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetlerinde şeffaflığın ve öngörülebilirliğin sağlanması önem taşımaktadır.

Kişisel veri işleme süreçlerinin şeffaf bir biçimde yürütülmesine yönelik olarak Kanun'un 16'ncı maddesinde öngörülen Veri Sorumluları Siciline/ VERBİS'e kayıt ve bildirim yükümlülüğü ile ilgili kişilerin kişisel verileri üzerinde üst düzeyde kontrole sahip olabilmeleri amaçlanmaktadır.

Mobil uygulamalar, uygulama mağazaları aracılığıyla dünya genelinde kullanıcıların hizmetine sunulmaktadır. Yurt dışında yerleşik sağlayıcıların sundukları mobil uygulamalar aracılığıyla Türkiye'deki kullanıcıların kişisel verilerinin işlenmesine sıklıkla rastlanmakta olup kullanıcıların kişisel verilerinin işlenmesinde bir şeffaflık mekanizması olan Veri Sorumluları Siciline kayıt yükümlülüğünün de yerine getirilmesi önem arz etmektedir.

Yurt dışında yerleşik sağlayıcıların sundukları mobil uygulamalarda; Türkiye'ye atıfta bulunarak mal ve hizmet sunulması, Türkiye'deki kişilere yönelik hizmetin verildiğini gösteren tanıtıcı açıklamalar yapılması, mal ve hizmet sunulmasında Türkçe dil seçeneği, Türkiye'ye ürün teslimatı seçeneğinin sunulması gibi hususların bulunması, mal ve hizmet sunumunda Türkiye'deki ilgili kişilerin hedeflenmesi; yahut davranışsal reklamcılık faaliyeti gerçekleştirilmesi, benzersiz tanımlayıcılar aracılığıyla çevrim içi takip yapılması ve pazarlama amacıyla coğrafi yerelleştirme faaliyetleri yürütülmesi

gibi işlemler gerçekleştirilmesi Türkiye'deki ilgili kişilerin davranışlarının izlenmesi anlamına gelecektir. Mobil uygulamalarda Türkiye'deki kullanıcıların hedeflenmesi veya davranışlarının izlenmesi söz konusu olduğunda, mobil uygulama aracılığıyla işlenen kişisel veriler bakımından Kanun'un 16'ncı maddesinde yer alan Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğünün de göz önünde bulundurulması önem taşımaktadır.

MOBİL UYGULAMALARDA ÇOCUKLARIN KİŞİSEL VERİLERİNİN İŞLENMESİ

Akıllı cihazların yaygınlaşarak kolay ulaşılabilir ürünler hâline gelmesi ile birlikte mobil uygulamaların çocuklar tarafından da sıklıkla kullanılmaya başlandığı dikkate alındığında, çocukların bilinç düzeyinin ve çocuklara ilişkin kişisel verilerin öneminin göz önünde bulundurulması suretiyle çocukların kişisel verilerine yönelik işleme faaliyetlerinin, diğer işleme faaliyetlerinden ayrı bir şekilde ele alınmasında fayda görülmektedir.

Bu nedenle, özellikle çocuklara yönelen veya çocuklar tarafından yaygın olarak kullanıldığı bilinen uygulamalar açısından, kullanıcıların yaşını doğrulayacak sistemler kurulması ve çocuklara yönelik işleme faaliyetlerinin ayrı bir politika ve prosedür takip edilerek gerçekleştirilmesi önerilmektedir.

Konu ile ilgili olarak Kurumumuz tarafından hazırlanmış olan "Çocukların Kişisel Verilerinin Korunması-Ürün ve Hizmet Geliştirenler Tarafından Dikkat Edilmesi Gerekenler" başlıklı dokümanın https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/db0b3f30-c636-4fcb-930a-bf8f2e524de8.pdf incelenmesinde fayda bulunmaktadır.

3. Kişisel Verilerin İşlenme Şartlarının Belirlenmesi

Kişisel verilerin işlenme şartları Kanun'un 5'inci maddesinde sayılmış olup buna göre maddede sayılan hâllerden en az birinin bulunması durumunda bireylerin kişisel verilerinin işlenmesi mümkündür. Bu çerçevede, anılan maddenin (1) numaralı fıkrasında kişisel verilerin, ilgili kişinin açık rızası olmaksızın işlenemeyeceği belirtilmekte ve devamındaki fıkrada;

a) Kanunlarda açıkça öngörülmesi,
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
(c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
(ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
(d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
(e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
(f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde,
ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu düzenlenmektedir.

Özel nitelikli kişisel verilerin işlenme şartları ise Kanun'un 6'ncı maddesinde hükme bağlanmıştır. Buna göre özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasak olup anılan maddenin (1) numaralı fıkrasında sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği; sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak 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 ilgilinin açık rızası aranmaksızın işlenebileceği düzenlenmektedir.

Mobil uygulamalar vasıtasıyla işlenen kişisel veriler açısından değerlendirildiğinde ise bu işlemeye dayanak oluşturacak işleme şartlarının belirlenmesi ve bu durumun gerekçeleri ile ortaya konulması beklenmektedir. İşlemeye dayanak oluşturacak şartların belirlenmesi, şeffaflığın sağlanması konusundaki yükümlülüğün yerine getirilebilmesi açısından da bir ön koşul niteliği taşımaktadır.

Konu ile ilgili olarak "Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler hakkında" Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/65 sayılı Kararının *(https://www.kvkk.gov.tr/Icerik/6717/2020-65)* incelenmesi faydalı olacaktır.

"Açık rıza" kişisel veri işleme şartlarından birisi olup veri işleme faaliyetinin gerçekleştirilmesinde, veri sorumlusu tarafından öncelikle diğer veri işleme şartlarından birisine dayanılıp dayanılamayacağı değerlendirilmeli ve bunlardan herhangi birisi bulunmuyorsa ilgili kişinin açık rızasının alınması yoluna gidilmelidir. Kanun'un 3'üncü maddesinde açık rıza, *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* şeklinde tanımlanmaktadır.

Mobil uygulamalar üzerinden gerçekleştirilecek kişisel veri işleme faaliyetlerinde, uygulamanın asıl işlevinin yerine getirilmesi için ihtiyaç duyulmayan kişisel verilerin işlenmesi durumunda kullanıcının açık rızasının alınması gerekliliği ortaya çıkabilecektir. Örneğin, bir kullanıcı tarafından talep edilen bir uygulamanın herhangi bir özelliği veya işlevi için kullanıcının konumuna erişilmesi gerekmeyen durumlarda, kullanıcı açık rıza vermediği sürece hedefli reklamcılık amaçları doğrultusunda kullanıcının konum verisi toplanmamalıdır. Benzer şekilde kullanıcılar, uygulamanın mikrofonlarına veya konumlarına erişim sağlaması gibi isteğe bağlı olan ve uygulamanın fonksiyonelliği açısından gerekli bulunmayan işlevlere yönelik izinleri devre dışı bırakmayı seçseler dahi uygulamanın kullanılabilmesine izin verilmelidir.

Diğer taraftan, kullanıcının aktif eylemiyle açık rızasının alınmasını sağlayacak mekanizmaların kurulması başta olmak üzere, Kanun'da öngörülen geçerlilik unsurlarını karşılayacak şekilde kullanıcıların açık rızasına başvurulması uygun olacaktır.

Konu ile ilgili olarak "Bir bankanın mobil uygulamalar üzerinden ilgili kişiye rızası dışında tanıtım iletileri göndermesi" hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarih ve 2021/361 sayılı Kararının *[https://www.kvkk.gov.tr/Icerik/7109/2021-361]* incelenmesinde fayda bulunmaktadır.

4. Veri Güvenliğinin Sağlanması

- Uygulamalar, tasarımdan itibaren mahremiyet *(privacy by design)* ve başlangıçtan itibaren mahremiyet *(privacy by default)* ilkeleri ile uyumlu şekilde tasarlanmalı ve kişisel verilerin korunmasını en üst düzeyde sağlayacak şekilde kullanıma sunulmalıdır. Zira bireyler tarafından gerçekleştirilecek ilave bir eyleme gerek duyulmaksızın mobil uygulamaların ilk kullanımında mahremiyet odaklı ayarların açık olması, hem kişisel verilerin işlenmesinde dürüstlük kuralına uyulması hem de kullanıcıda güven tesis edilmesi bakımından büyük önem arz etmektedir.

- Mobil uygulamaların kullanıldığı cihazlara yetkisiz erişimler gerçekleştirilmesini önlemek adına cihazlarda kimlik doğrulama yöntemlerinin kullanılması sağlanmalıdır. Bununla birlikte, aynı anda farklı cihazlardan oturum açılması bakımından kullanıcılara yönelik kontrol mekanizmaları oluşturulmasında fayda bulunmaktadır.

- Kullanıcılar, mümkünse çok faktörlü kimlik doğrulama yöntemlerinin kullanılmasına teşvik edilmelidir.

- Mobil uygulamalara erişimlerde kullanıcılar tarafından güçlü parolalar oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesi sağlanarak uygun bir parola güvenliği politikası işletilmelidir. Kullanıcılar tarafından yeni parola oluşturulurken daha önce kullandıkları eski parolaların yeniden kullanılmasının önüne geçilmesi faydalı olacaktır.

- Parolalar, yeterli güvenlik önlemleri alınarak saklanmalıdır. Siber saldırı riskine karşı parolaların güncel "özet/karma*(hashing)*"[15] fonksiyonlarından geçirilerek muhafaza edilmesi önerilmektedir.

- Düzenli olarak yama yönetimi ve yazılım güncellemesi süreçleri gerçekleştirilmelidir. Mobil uygulamalardaki açıkların ve zafiyetlerin kapatılması adına yazılımların güncel tutulması, uygulama güvenliğinin sağlanmasına yardımcı olacaktır.

- Geliştirilen mobil uygulamaların yayımlanmasından önce yazılım testlerinin uygun şekilde gerçekleştirildiğinden emin olunmalıdır. Bu kapsamda, geliştirilen uygulamaların ilk kullanımına çıkılmasından önce yazılım testlerinden eksiksiz ve başarılı bir şekilde geçildiği güvence altına alınmalıdır.

15 Özet/Karma *(hashing)* algoritmalar, değişken uzunluktaki verileri okunmaz hâle getirerek sabit uzunluktaki verilere haritalayan algoritmalar olarak tanımlanabilmektedir.

- Uygulama güvenliğinin, tasarım aşamasında başladığının bilincinde olunmalı ve güvenli yazılım geliştirme stratejileri yürütülmelidir.

- Kullanıcıların mobil uygulamalara ilişkin hesap girişlerinde başarısız giriş sayısı sınırlandırılmalıdır. Bot saldırılarına bir önlem olarak kullanıcı girişi olan sayfalarda CAPTCHA, dört işlem vb. gibi yöntemler tercih edilmelidir.

- Uygulamalar yayımlanmadan önce hedeflenen işletim sistemlerinin veri koruma ve güvenlik özellikleri dikkate alınmalıdır. Bu kapsamda, risk değerlendirmesi yapılmasında fayda görülmektedir.

- 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 kullanılmalıdır. Kişisel verilerin mobil cihazlarda muhafaza edildiği durumlarda, kişisel verilerin etkili bir şekilde şifrelenmesi yoluyla kişisel veri güvenliğinin sağlandığından emin olunmalıdır.

KAYNAKLAR

Achara, J.P./Acs, G./Castelluccia, C.: On the Unicity of Smartphone Applications, Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society, 2015, https://api.semanticscholar.org/CorpusID:15723203.

European Union Agency for Network and Information Security (ENISA): Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR, 2017, https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

Office of the Privacy Commissioner of Canada/Office of the Information and Privacy Commissioner of Alberta/ Office of the Information&Privacy Commissioner for British Columbia: Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps, 2012, https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/.

Pham, A.: Privacy-Enhancing Technologies for Mobile Applications and Services, 2019, https://www.semanticscholar.org/paper/Privacy-Enhancing-Technologies-for-Mobile-and-Pham/8be301a85c445ef365a03857ca473e254922cfec

World Intellectual Property Organization (WIPO): A Guide to Data Protection in Mobile Applications, 2021, https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU