



KVKK Kapsamında Apple Touch ID ve Face ID ile Biyometrik Veri İşleme Faaliyeti

HAZIRLAYANLAR

Av.Nagihan Aydın

Av.Abdullah Erkam Yılmaz

03

**KVKK
Kapsamında
Apple Touch ID
ve Face ID ile
Biyometrik
Veri İşleme
Faaliyeti**



04

**Veri İşleyen
Veri Sorumlusu
Ayrımı**



05

**Biyometrik
Verinin Yurt Dışına
Aktarılması
Bakımından**



06

**İşveren Tarafından
Aydınlatma Yapılması
ve Açık Rıza Alınması
Bakımından**



KVKK Kapsamında Apple Touch ID ve Face ID ile Biyometrik Veri İşleme Faaliyeti

Apple ürünleri Touch ID ve Face ID gibi teknolojileriyle yüz tanıma ve parmak izi algılama sistemleri sayesinde iPhone, iPad ve MacBook'larda kilitli ekranların açılması, iTunes Store, App Store ve iBooks Store uygulamalarından satın alımların gerçekleştirilmesi, bazı uygulama geliştiricilerinin uygulamalarına giriş yapılmasını sağlaması gibi pek çok özelliği sayesinde güvenli kullanım sağlamaktadır. Bu ürünleri kullanan kişiler açısından Touch ID neredeyse dijital kimlik haline gelmiştir. **Peki bu ürünleri çalışanlarına kullandıran işverenler bakımından bir aydınlatma yükümlülüğü doğmakta mıdır? Bu durumda biyometrik veri alımına ilişkin açık rıza alınması gerekmekte midir? Kişisel verilerin yurt dışına aktarımı konusunda ayrıca bir açık rıza alınacak mıdır?**

İşverenler, çalışanlarının kişisel verilerini Kanun'da belirtilen ilkelere uygun olarak işlemek zorundadır. Aksi bir yaklaşım **yüklü miktarda idari para cezası** kesilmesine sebep olmaktadır. Bir görüşe göre çalışan, Touch ID kullanmadan yalnızca şifre belirlenmesi yöntemiyle sistemlere giriş yapılabildiğinden dolayı işveren zorunlu kılmadığı müddetçe kendi isteğiyle bu verileri kaydetmek suretiyle giriş yapmış olacağından **işverenin sorumluluğu doğmayacağı** yönündedir. Diğer görüş ise işverenin zorunlu kılıp kılmadığına bakılmaksızın biyometrik verinin işlenmiş olduğu ve buna göre önlem ve tedbirlerin alınması gerektiği yönündedir.



Veri İşleyen - Veri Sorumlusu Ayrımı

Parmak izi ve yüz tanıma sistemlerinin özel nitelikli biyometrik veri olduğu hususunda bir görüş ayrılığı bulunmamaktadır. Apple ürünleri söz konusu olduğunda bu verilerin yurt dışına aktarılıp aktarılmadığı ise incelenmesi gereken bir sorudur. Apple Inc., ürünleri aracılığıyla hiçbir şekilde biyometrik veri toplamadığı yönünde bir açıklama yapmıştır. Öncelikle işverenin veri sorumlusu-veri işleyen kategorilerinden hangisine girdiğinin tespit edilmesi gerekmektedir. Yasal düzenlemelere göre veri sorumlusu; **“Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi”** ifade etmektedir. Veri işleyen ise; “Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi” ifade etmektedir. Mevcut ilişkilerde işverenin, veri sorumlusu-veri işleyen kategorisinden hangisine girdiğini tespit etmek çetrefilli bir vaziyet olabilir. Söz konusu tespit, Avrupa Veri Koruma Kurulu’nun konuya ilişkin hazırlamış olduğu en yeni kılavuz olan **“Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1”** baz alınarak yapıldığında mesele biraz daha aydınlığa kavuşmaktadır.

Önceki paragraflarda tespit edildiği üzere **Apple ürünlerinin TouchID vasıtasıyla kullanılması durumunda üçüncü kişi olan Apple Inc. veri işleme süreçlerine dahil olmamaktadır.** Bu noktada işverenin yasal düzenlemeye göre veri sorumlusu kapsamına girip girmediği, kanuni dayanaklar çerçevesinde yapmakla yükümlü olduğu görevini yerine getirmek amacıyla veri işleme faaliyetinin gerekli olup olmadığı ve veri sorumlusu sıfatıyla belirli bazı kararları alıp almadığı değerlendirilmek **suretiyle bir sonuca varılması gerekmektedir.**

Veri sorumlusunun alabileceği kararlar:

- Verinin hangi amaçla veya amaçlarla işlenebileceği,
- Hangi kişisel verinin toplanacağı ve işleneceği,
- İşlenen verinin hangi kategorideki bireylere ilişkin olacağı,
- Verinin paylaşılıp paylaşılmayacağı ve kim veya kimlerle paylaşılacağı,
- Kişisel verinin ne kadar süreyle saklanacağı.

Sayılan kararları alan gerçek veya tüzel kişi, veri sorumlusu olarak kabul edilecektir. Kişisel veri işleme sürecine üçüncü tarafların dahil olması halinde ise **ortak veri sorumluluğunun bulunup bulunmadığı değerlendirmeye alınabilecektir.**

Gerçek veya tüzel kişi, veri işleme faaliyetini başkası adına ve onun talimatları doğrultusunda yapmakta veya veri işleme faaliyetini başkası adına ve yalnızca başkasının talimatları doğrultusunda yapmakta ve işleme amaçları ve araçları hakkında kendi insiyatifiyle karar almamaktaysa **veri işleyen olarak tanımlanabilecektir.**

Bu ayırmada veri işlemenin amaçları ve araçları hakkında kimin karar verdiği konusunda belirsizlik bulunuyor ise veri işleyen gerçek veya tüzel kişinin **veri sorumlusu veya veri işleyen olup olmadığı sayılan durumlar kontrol edilerek anlaşılabilir:**

Veri Sorumlusu Olduğuna İşaret Eden Durumlar	Veri İşleyen Olduğuna İşaret Eden Durumlar
- İşlemeden bir fayda elde edilmesi veya menfaat sağlanması, - İşleme faaliyetinin bir bölümünün veya sonucunun ilgilendirdiği kişiler hakkında kararlar verilmesi, - İşleme faaliyetlerinin kuruluşun görev veya aktivitelerinin doğal bir gereği olarak değerlendirilip kişisel verilerin korunması açısından sorumluluğa yol açması, - Veri işleme faaliyetlerinin; çalışan, müşteri, üye vb. ilgili kişilerle olan hukuki ilişki bağlamında gerçekleştirilmesi, - Kişisel verilerin işlenmesinde tam yetki sahibi olması, - Kişisel verilerin işlenmesinde bir başka yapının kişisel verileri kendi adına işlemesine yetki verilmesi.	- Kişisel verilerin başka bir tarafın amaçları için verilen talimatlara göre işlenmesi ve işleme için kendine ait bir amacının olmaması, - Üçüncü bir gerçek veya tüzel kişi tarafından, ilgili sözleşme hükümlerine ve talimatlarına uygun olarak hareket edildiğinden emin olmak için kontrol ediliyor olması, - İşleme faaliyeti kapsamında, hizmet sunmak için kendi firmasının dışında herhangi bir işleme amacının bulunmaması, - Belirli işleme faaliyetlerini yürütmek için üçüncü bir taraf adına ve bu tarafın belgelendirilmiş talimatları doğrultusunda veri işlemek için görevlendirilme.

Yüz tanıma ve parmak izi sistemi yalnızca kaydedildiği **Apple cihazları özelinde** encrypt edilerek (şifrelenerek) saklanmaktadır. Bu konu encrypt edilen biyometrik verilere işverenin ulaşma imkanı bulunup bulunmamasına göre şekillenecektir. İşveren bu verilere ulaşabilmekte midir? Bir görüşe göre cihazın içerisine şifrelenmiş şekilde kaydedilen veriyi işveren başka bir yerde kullanamadığından veri kaydedilmesi söz konusu değilken diğer görüşe göre **çalışanın biyometrik verisi işveren tarafından başka yerde kullanılamasa da cihaza kaydedildiğinden veri imha talebi yine işverene yapılacak olup bu da işverenin sorumlu olduğu anlamına gelecektir.**

Biyometrik Verinin Yurt Dışına Aktarılması Bakımından

Apple Inc. biyometrik verilerin işlenmesi ile kişisel veri ihlali olup olmadığı konusunda yaptığı açıklamada “**Biyometrik veriler kullanıcının sahip olduğu ve kontrol ettiği Apple aygıtındaki bellekte kalır.**” demektedir. Bu durumda çalışana verilen Apple ürünlerine kaydedilen biyometrik veriler yurt dışına aktarılmamakta, yalnızca söz konusu cihazlarda saklanmaktadır. Bu durumda biyometrik veri işlendiği kabul edilsin ya da edilmesin kişisel verilerin yurt dışına aktarımına dair **açık rıza alınması gerekmemektedir.**

İşveren Tarafından Aydınlatma Yapılması ve Açık Rıza Alınması Bakımından

İşveren tarafından şifre koruma faktörünün ve güvenliğin artırılması gerekçe göstererek çalışanın belirleyeceği şifrenin yanında yüz tanıma ve parmak izi sistemine biyometrik verilerini girmesini istemesi durumunda dahi kişisel verilerin işveren tarafından veya Apple Inc. tarafından işlenmediği söylenebilir. Bu konuda cihazların üreticisinden gelen açıklamaya itibarla işverenin biyometrik veri işlemediği ve bu sebeple çalışana aydınlatma yapması veya **açık rıza alması gerekmediği savunulabilir.**

Diğer görüşe göre ise işverene ait bir cihazda, çalışanın biyometrik verilerinin çalışan iş yerinden ayrıldıktan sonra dahi kayıtlı kalması durumunda işverenin konumuna göre veri sorumlusu veya veri işleyen olarak sorumluluk alması gerektiğidir. Değilse çalışan biyometrik verilerinin silinmesi için kime karşı talepte bulunacaktır?

Apple Inc.'in yaptığı açıklamaya göre kaydedilen biyometrik veriler cihazdan dışarı çıkmadığından dolayı bu veriler yalnızca söz konusu cihazlarla sınırlı olmak üzere kaydedilmektedir. **Aynı iCloud Mail hesabıyla dahi başka bir cihazda oturum açıldığında başka bir cihazda kaydedilen biyometrik veriler ile giriş yapılması mümkün olmamaktadır.**

Sonuç olarak KVKK kapsamında işverenin, çalışana Apple ürünleri kullanırmak suretiyle özel nitelikli kişisel veri olan biyometrik verileri işleyip işlemediği konusunda iki farklı görüş bulunmakta ve konunun aydınlanabilmesi için **şifreleme (encryption) ve Apple cihazları konusunda uzman kişilerin de görüşleri alınarak bir karara varılması gerekmektedir.**

Teşekkürler



Abdullah Erkam Yılmaz
Kurucu Avukat

İletişim:

aeylegal.com
erkam@aeylegal.com

Nagihan Aydın
Avukat

İletişim:

aeylegal.com
nagihan@aeylegal.com



Sorularınız ve görüşleriniz için
bizimle iletişime geçebilirsiniz.