ERCİYES AKADEMİ, 2022, 36(3), 1424-1445
https://doi.org/10.48070/erciyesakademi.1150085

SAĞLIK VERİLERİNİN İŞLENMESİNDE AYDINLATMA YÜKÜMLÜLÜĞÜ*

Miray ÖZER DENİZ[a]

Özet

Kişisel sağlık verileri, Kişisel Verilerin Korunması Kanunu (KVKK) m. 6 uyarınca özel nitelikli kişisel veridir. Kişisel verilerin işlenmesinin hukuka uygunluk nedenlerinin başında ilgili kişinin işleme faaliyetine yönelik açık rıza vermesi gelmektedir. Açık rıza gerekmeksizin verilerin işlenebilmesi hali ise istisna olarak düzenlenmiştir. Kişisel verilerin işlenmesi bakımından geçerli olan rıza, aydınlatılmış rızadır. İlgili kişinin sağlık verisinin işlenmesine yönelik verdiği rızanın geçerli olabilmesi için açık rıza beyanından önce aydınlatılmış olması gerekir. Aydınlatma yükümlülüğü, geçerli bir rızanın şartı olmakla birlikte ayrıca ilgili kişinin sahip olduğu düzeltme, silme veya itiraz hakları gibi bağlantılı diğer haklarının kullanımı için de gereklidir. İlgili kişinin aydınlatılması, KVKK m. 10'da veri sorumlusunun yükümlülüklerinden biri olarak düzenlenmiştir. KVKK m. 10'un uygulanmasına ilişkin usuller Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde (Tebliğ) yayımlanmıştır. Çalışmamızda, KVKK ve Tebliğ çerçevesinde, sağlık verilerinin işlenmesinden önce veri sorumlusu olan doktor veya hastanenin ilgili kişiyi aydınlatma yükümlülüğü, şekli ve maddi unsurları ile bu yükümlülüğe uyulmamasının hukuki sonuçları incelenecektir.

Anahtar Kelimeler: Sağlık verileri, Aydınlatma yükümlülüğü, Özel nitelikli kişisel veriler, Kişisel verilerin işlenmesi.

✵ ✵ ✵

THE OBLIGATION TO INFORM IN PROCESSING PERSONAL HEALTH DATA

Abstract

Personal data concerning health is deemed to be special personal data according to Personal Data Protection Code Art 6. It is prohibited to process special categories of personal data without the explicit consent of the data subject. In Art 6/3 exceptions that such data can be processed without explicit consent are regulated. One of the conditions for processing personal data is explicit consent which should be given after being informed. The obligation of the data controller to inform is regulated in Art. 10. This obligation is compulsory not only for explicit consent but also for the application of other related rights such as correction, deletion or objection rights of the data subject. The details of obligation of data controller to inform is regulated in Communique On Principles And Procedures To Be Followed In Fulfilment Of The Obligation To Inform. In this study, the

*Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Doktora programı kapsamında hazırlanan "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk" adlı tezden türetilmiş makaledir.

[a] Arş. Gör. Dr., Çukurova Üniversitesi, Hukuk Fakültesi, Medeni Hukuk Bölümü, ozermiray@yahoo.com

Makale Geliş Tarihi: 28.07.2022, Makale Kabul Tarihi: 19.09.2022

obligation of the data controller to inform before processing of health data, form of the obligation and the legal sanctions of the breach of the obligation will be examined in the aspects of the Personal Data Protection Law and the Communique.
Keywords: Personal health data, Obligation of data controller to inform, Special category of personal data, Data processing.

❋ ❋ ❋

Giriş

Kişisel veri, Kişisel Verilerin Korunması Kanunu (KVKK) m. 3'te kimliği belli ya da belirlenebilir bir gerçek kişiye ait her türlü veri olarak tanımlanmıştır. Kanuni tanımdan hareketle bir verinin kişisel veri olarak tanımlanabilmesi için üç unsurun birlikte var olması gerekir (Özer Deniz, 2022, s. 45). Söz konusu üç unsur, kişi, veri ve kişi ile veri arasında bağlantı kurulabilmesidir.

Birinci unsur olan kişi, KVKK'ya göre, sadece gerçek kişidir. Kişi, hak sahibi hukuk süjesidir (Oğuzman vd., 2014). KVKK, sadece gerçek kişileri kapsama almıştır. İkinci unsur olan veri, bir olay, bir kişi veya durum ile ilgili tüm bilgilerin genelidir (Fry, 1983, s. 5). Verinin, kanun kapsamında değerlendirilmesi noktasında, doğru, yanlış, objektif ya da sübjektif olmasının bir önemi yoktur (Ayözger Öngün, 2019; Aşıkoğlu, 2018; Özer Deniz, 2022). Kişiye ilişkin bir bilgi olması yeterlidir. Dolayısıyla, örneğin, kişinin yaşının hasta kayıt sistemine sehven hatalı olarak işlenmesi verinin, kişisel veri olarak kabul edilmesini etkilemez.

Son olarak, veri ile kişi arasında bağ kurulabilmesi gerekir. Aksi halde veri, kişisel veri değil anonim veri olacaktır. Örneğin, bir hastane kayıt sisteminde birden çok Emine isminin bulunması ismi her Emine olan kişinin kişisel verisi olmayacaktır. Zira bu isim ile kişi arasındaki bağ kurulamamaktadır. Ne zaman ki soyadı, yaşı, hastalık bilgisi gibi ek veri işlemeleri ile bir kişi ile bağlantı kurulursa o halde Emine ismi kişisel veri olarak kabul edilir.

Kişisel veriler, genel kişisel veriler ile özel kişisel veriler olarak iki gruba ayrılmıştır. Genel nitelikteki kişisel veriler, sınırlı sayı ilkesi olmaksızın, kişi ile ilişki kurabilen her türlü verilerdir (Özer Deniz, 2022, s. 46). Bu kapsamda; fotoğraf, adres, telefon numarası, elektronik posta adresi, banka hesap numarası, yaşı, mesleği, eğitim bilgileri gibi veriler genel nitelikteki kişisel verilerdir.

Özel nitelikli kişisel veriler ise KVKK m. 6'da sayılan verilerdir. KVKK, "*Özel Nitelikli Kişisel Verilerin İşlenme Şartları*" başlıklı 6. maddenin 1. fıkrasında özel nitelikli kişisel verilerin tanımını yaparak hangi verilerin özel nitelikli veri olduğunu tek tek saymıştır. Maddeye göre, 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 özel nitelikli kişisel veridir. Bu veriler, kanunda sınırlı olarak sayıldığından yorum yapılarak genişletilemezler (Özer Deniz, 2022, s. 51).

A. KİŞİSEL SAĞLIK VERİLERİ

Çalışmamızın konusunu oluşturan özel nitelikli kişisel verilerden sağlık verileri KVKK'da tanımlanmamıştır. Kişisel Sağlık Verileri Hakkında Yönetmelik m. 4'e göre, kişisel sağlık verisi *"Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileridir*". Bu tanıma göre, sağlık verisi, bir kişinin tanı, teşhis ve tedavisi sırasında başta sağlık personeli tarafından elde edilen her türlü verisidir (Abik, 2018; Orak, 2019; Yılmaz, 2019).

Avrupa Birliği Veri Koruma Tüzüğü (Tüzük) m. 4/15'te ise kişisel sağlık verisi, "*Sağlık hizmetlerinin sağlanması da dâhil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir*." şeklinde tanımlanmıştır. Dünya Hekimler Birliği, Sağlık Veri Tabanları ile İlgili Etik Düşünceler Bildirgesi'nde kişisel sağlık verisini "*bireyin kimliğini ortaya koyan fiziksel ve mental sağlığı ile ilgili kayıtlı tüm bilgi*" olarak tanımlar. 03.12.2003 tarihli 5013 sayılı kanun ile Türkiye tarafından kabul edilen İnsan Hakları ve Biyotıp Sözleşmesinin *"Özel yaşam ve bilgilendirilme hakkı*" başlıklı 10. maddesinde, "*Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir."* denilmiştir. AB Temel Haklar Şartı'nın 8. maddesinde *"Kişisel Bilgilerin Korunması Hakkı"* başlığıyla, 13. maddesinde *"Sağlık Hakkı"* başlığıyla kişilerin sağlıklarına ilişkin verilerinin korunması amaçlamıştır.

Sağlık verileri olarak değerlendirilecek öncelikli veriler, hastalara yapılan tüm müdahaleleri içeren tıbbi kayıtlardır (Somer, 2011; Taşatan, 2011). Hastaya yapılan her müdahalenin kayıt altına alınması, hem hastaya yapılacak müdahalenin kontrolünü sağlamak ve mükerrer müdahalenin yapılmasını önlemek hem de doktorun kendi hukuki sorumluluğu açısından gereklidir (Dülger, 2015; Özer Deniz, 2022).

Tıbbi kayıtlar, sağlık personeli tarafından hazırlanan ve hastalıkların teşhis ve tedavisi amacına hizmet eden tıbbi doküman, dokümantasyon, tıbbi belge, hasta giriş kaydı, sağlık belgeleri ve reçete gibi kişinin sağlığına ilişkin bilgilerin yer aldığı kâğıt veya elektronik ortama kaydedilmiş belgelerdir (Orak, 2021, s. 11). Tıbbi kayıtlarda yer alan hastanın kimliği, hastalığın öyküsü, teşhis ve tedaviye ilişkin veriler, epikriz raporu gibi bilgiler, ilgili kişinin sağlığına ilişkin kişisel verileridir (Hakeri, 2015; Taşatan, 2011).

Yukarıda belirttiğimiz gibi veriler, fiziksel veya elektronik ortamda muhafaza edilebilir. Bu kapsamda, elektronik sağlık kayıtları (e-sağlık) ve dijital hastanelerde kullanılan veriler, kişisel sağlık verileri olacaktır. Elektronik sağlık kayıtları, kişilerin ilgili elektronik sistemler kullanılarak saklanan, iletilen, erişilen, ilişkilendirilen ve işlenen her türlü verileri olarak tanımlanır (Aldaş, 2018, s. 112). Şu anda, kişisel sağlık verileri, Medula, E-nabız, Gebliz, Aşı-net, Acil Servis Ünitesi İntihar Girişimi Kayıtları, Ulusal Sağlık Bilgi Sistemine kaydedilmektedir. Bu kayıtlar neticesinde, ilgili kişilerin sağlık verilerine, doktorlar, konsültanlar, diğer sağlık çalışanları, sağlık kurumlarındaki idari personel, laboratuvar çalışanları, eczaneler, Sosyal Güvenlik Kurumu, Sağlık Bakanlığı, Maliye, Adli makamlar ve Türkiye Sigorta Birliği erişebilmektedir. Doktrinde E-nabız uygulamasının normlar hiyerarşisine uygun

olmadığı ve genelge ile kanuna aykırı düzenleme yapıldığını düşünen yazarlar da bulunmaktadır. (Abik, 2018; Özer Deniz, 2022).

E-sağlık, Dünya Sağlık Örgütü tarafından enformasyon ve iletişim teknolojilerinin sağlık amacıyla kullanılması olarak tanımlanır (http://www.who.int/ehealth/about/en). Dijital hastaneler ise kişilerin sağlık hizmetlerine erişimi, hastane ve sağlık masraflarının azalması, kişilere en uygun teşhis ve tanı için kullanılmaktadır (Küzeci, 2018, s. 477). Bunun yanında klinik karar destek sistemleri de sağlık verilerini işleyerek, doktrin ve uygulamadaki tüm tanı ve teşhisler ile karşılaştırarak hastanın somut olayına uygulanabilir en etkili çözüm yolunun bulunmasına yardım eder (Aldaş, 2018, s. 112). Bu sistem, doktorun ilgili hastaya en uygun tanı ve teşhisi koymasına katkı sağlar (Sütçü & Tosyalı, 2016, s. 100). Örneğin, New York'ta geliştirilen bir projede, 2 milyon sayfalık bilimsel makale ve 600.000 bilimsel veri birkaç dakika içinde taranmış ve kanser hastalarına yönelik tedavi önerileri sunulmuştur (Sütçü & Tosyalı, 2016, s. 106).

Sağlık verileri, teknolojideki gelişmeler ile birlikte, geçmişe nazaran çok daha farklı ve fazla şekilde işlenmektedir. Artık sağlık verileri, yalnızca sağlık hizmetleri sırasında değil, farklı amaçlarla veri işlenmesi sırasında da elde edilebilir (Küzeci, 2018; Özer Deniz, 2022). Örneğin, kişinin akıllı saatinin veri aktarımı, kilo ve ovulasyon takibi yapan akıllı cihaz uygulamaları, belli hastalıklara destek gruplarına üyelikleri, sağlık ürünlerine ilişkin alışveriş verileri gibi veri işleme faaliyetleri sonucunda da sağlık verileri elde edilebilir (https://autoriteitpersoonsgegevens.nl). Mağazaların sadakat kart uygulamaları, alışveriş tercihleri ve sıklığından yola çıkarak pek çok veri elde edebilir. Örneğin, Amerika Birleşik Devletleri'nde bir perakende alışveriş merkezi, bir kullanıcının doğum kontrol ürünleri satın almayı bırakıp hamilelik ve bebek bakım ürünleri almaya başlamasından, tüketicinin hamile kaldığını ve yaklaşık doğum zamanını tahmin edebilmiştir (www.forbes.com, 2012). Buradan çıkacak sonuç ile aslında giyilebilir teknolojiler, nesnelerin interneti ve çevrimiçi veya çevrimdışı davranışsal reklamcılık uygulamalarıyla birlikte pek çok veri kolaylıkla elde edilebilir (Küzeci, 2018; Özer Deniz, 2022).

Bunun yanında, verilerin aktarılması ve verilere erişim de artık daha kolaydır. Örneğin, hastalar e-nabız sistemi üzerinden sağlık verilerine erişebilmekte; bunları doktorlara yetki vererek paylaşabilmektedir. Uzaktan tedavi yöntemleri de sağlık verilerinin paylaşılmasını ve aktarılmasını kolaylaştırmaktadır. Uzaktan sağlık hizmetleri, ülkemizde Uzaktan Sağlık Hizmetlerinin Sunumu Hakkında Yönetmelik'te düzenlenmiştir. İlgili Yönetmeliğin 12. maddesinde kişisel verilerin korunmasına ilişkin hüküm yer almaktadır.

Sağlık verilerinin, genel nitelikli verilerden ayrılıp sağlık verisi olarak tanımlanabilmesi her zaman kolay olmamaktadır. Bu durum sadece sağlık verileri için değil, diğer özel veri türleri bakımından da geçerlidir. Örneğin, siyahi bir kişinin fotoğrafından kişinin ırk verisine ya da baş örtüsü ile çekilen bir fotoğraftan dini görüşüne ilişkin özel nitelikli verisine de ulaşılabilir. Bu durumda, sözü edilen bu fotoğrafın genel nitelikli veri mi özel nitelikli veri mi olduğunun kabulü için fotoğrafın çekilme amacına bakılması gerekir. İngiltere'de Naomi Campbell v MGN davasında Lordlar Kamarası, Campbell'in fotoğraflarının ırkını belli eden özel nitelikli veri olarak değerlendirilip değerlendirilemeyeceğini tartışmıştır. Bu olayda mahkeme, fotoğrafın çekilme amacının mankenin ırkını vurgulamak olmadığını

göz önüne alarak fotoğrafların özel nitelikli veri olarak kabul edilemeyeceğine karar vermiştir (Özer Deniz, 2022, s. 128).

Bazı veriler, genel nitelikli veri olarak kabul edilmekle birlikte başka veriler ile birlikte değerlendirildiğinde sağlık verisi haline dönüşebilir. Örneğin, kişinin sosyal medya hesabında paylaştığı duygu durumunu belirten ifadeler bile toplanıp başka veriler ile birleştirilerek kişinin ruh sağlığına ilişkin veri olarak kaydedilebilir. Bazı veriler ise genel nitelikli veri olmakla birlikte sağlığa ilişkin bilgiler de sağlayabilir. Örneğin, bir kişinin fotoğrafı genel nitelikli veridir. Buna karşın, kişinin gözlük takarken çekildiği bir fotoğraftan ilgili kişinin göz sağlığına ilişkin bilgiye; down sendromlu bir kişinin fotoğrafından sağlık durumuna ilişkin veriye de ulaşılabilir.

Belirtmek gerekir ki ilk bakışta sağlık verisi gibi gözükmeyen ya da ilave veri kombinasyonları yardımıyla sağlık verisine dönüşen verilerin doğru tanımlanması, öncelikle bu verilerin korunması için gereklidir. Zira genel nitelikli veri ile sağlık verisi ayrımı yapılamazsa sağlık verileri, genel nitelikli verilerin koruma alanına girer. Bu da sağlık verilerinin özel nitelikli veri olarak korunamamasına sebep olur. Bu gibi durumlarda ise sağlık verilerinin özellikle profilleme ya da pazarlama amacıyla kullanılmasının önünü açılır (Özer Deniz, 2022; Tayan, 2017).

B. SAĞLIK VERİLERİNİN İŞLENMESİ VE HUKUKA UYGUNLUK HALLERİ

1. Kişisel Verilerinin İşlenmesine İlişkin Genel Düzenlemeler

Genel nitelikli kişisel verilerin işlenmesinin hukuka uygunluk halleri KVKK m. 5'te, özel nitelikli kişisel verilerin işlenmesinin uygunluk halleri ise KVKK m. 6'da düzenlenmiştir. Sağlık verilerinin bu şekilde farklı maddede düzenlenmesinin nedeni, ilgili kişinin iş ve sosyal hayatını etkileyerek ayrımcılığa uğramasına, maddi ve manevi olarak zarar görmesine oldukça müsait olmasıdır.

KVKK'ya göre, hem genel nitelikli hem de özel nitelikli kişisel veriler kural olarak kişinin açık rızası olmaksızın işlenemez (m. 5/1, m. 6/2). Bu nedenle özel nitelikli kişisel verilerden olan sağlık verileri de kural olarak açık rıza olmaksızın işlenemez. TDK'ya göre rıza, "onama, razı olma" anlamına gelmektedir (TDK, 2022). Hukuki olarak rıza ise kişinin, hukuki mal veya şahıs varlığına yapılan müdahaleye razı olmasıdır (Develioğlu, 2016, s. 55; Polat, 2019, s. 6). Kişisel verilere verilecek rıza ise kişisel verilerin işlenmesine razı olma ve bunu onama anlamına gelecektir.

İlgili kişinin açık rızasının geçerli olabilmesi için rıza beyanı öncesinde aydınlatma yükümlülüğünün yerine getirilmesi gerekir. Daha sonra rızanın belirli bir konuya ilişkin olup özgür iradeyle verilmesi gerekir. KVKK m. 6'da kişisel sağlık verilerinin açık rıza aranmaksızın işlenebileceği haller de belirlenmiştir.

Kişisel verilerin işlenmesini hukuka uygun hale getirecek rıza beyanının geçerli olması için öncelikle verilecek rızanın, hukuka, ahlaka ve kanunlara aykırı olmaması gerekir (Özer Deniz, 2022, s. 96). Bunun yanında, ilgili kişinin rıza gösterilecek konu ile ilgili önceden bilgilendirilmiş olması, özgür iradesiyle rıza göstermesi ve rıza verilmesi istenen hususun meşru ve sınırlarının belli olması gerekir (Ayözger Öngün, 2018; Braun, 2018; Dülger, 2019; Ferretti, 2012; Özer Deniz, 2022).

Öncelikle, ilgili kişinin rıza beyanından önce rıza göstereceği konuya ilişkin bilgilendirilmiş olması, bir başka deyişle aydınlatma yükümlülüğünün yerine getirilmiş olması gerekir. **(**Ayözger Öngün, 2018; Dülger, 2019; Küzeci, 2019; Özer Deniz, 2022). İlgili kişinin, onay vermeden önce işleme faaliyetlerinin hukuki dayanağını ve amacının ne olduğunu belirli ve açık ifadelerle bilmesi gerekir (Kişisel Verileri Koruma Kurumu (KVKK), 2019). Bu şekilde, kanuni dayanağı olmayan veya amacın anlaşılamadığı durumda kişi rıza göstermekten kaçınabilir.

KVKK 10. maddesinde veri sorumlusuna ilgili kişiyi aydınlatma yükümlülüğü yüklenmiş ve bu aydınlatmanın ifasına ilişkin usuller Kişisel Verileri Koruma Kurumu'na dayalı olarak çıkarılan "*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği*'nde yayımlanmıştır. Bu Tebliğ'de bildirimin yapılmasına ilişkin bir şekil şartı öngörülmemekle birlikte ispat kolaylığı sağlaması adına yazılı olarak yapılması yararlı olacaktır.

Ayrıca aydınlatmanın anlaşılabilir, sade ve teknik terimlerden uzak bir ifade ile yapılması, ilgili kişi tarafından anlaşılmasını kolaylaştıracaktır (Custers vd., 2013; Özer Deniz, 2022). Aydınlatmanın muğlak ve belirsiz içeriklerden ziyade net ve sınırlarının belli olması gerekir.

2. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin İlgili Kişinin Açık Rızası Aranmaksızın İşlenmesi

KVKK'nın 6. maddesinin 3. fıkrası, "Sağlık ve cinsel hayata ilişkin kişisel veriler 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 işlenebilir." şeklindedir.

Madde metninden anlaşılacağı üzere kanun koyucu, açık rıza olmaksızın sağlık ve cinsel hayata ilişkin verilerin işlenmesin bakımından istisnayı verinin türü, veriyi işleyen kişi, veri işlemenin amacı ve alınan önlem olmak üzere dört esas üzerinden düzenlemiştir.

a. Sağlık ve cinsel hayata ilişkin veri olması

İstisna kapsamına yalnızca sağlık ve cinsel hayata ilişkin veriler dahil edilmiştir. Esasında sağlık ile cinsel hayata ilişkin veriler (hatta her ne kadar kanuni düzenlemede yer almasa da genetik veriler) birbiriyle ilişkili verilerdir. Örneğin çoğu durumda, cinsel bir hastalığa ilişkin veri her iki veri türüne de dâhil olabilmektedir. Dolayısıyla, her iki verinin birlikte istisna kapsamında olması isabetli olmuştur.

Her iki verinin de özel nitelikli veri olarak kabulü ile işlenme şartlarının diğer veri türlerinden daha ayrıntılı olarak düzenlenmesinin nedeni, ilgili kişilerin bu verilerinin ortaya çıkmasının doğurduğu risktir. Bu veriler, ilgili kişilerin toplum içinde ayrımcılık yaşamasına neden olabilecek veriler. Bu duruma istinaden Avrupa İnsan Hakları Mahkemesi (AİHM), cinsiyet belirleme, isim ve cinsel tercih ve cinsel hayatın Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesi kapsamında korunması gerektiğine ilişkin karar vermiştir (Bknz örneğin, Laskey, Jaggard ve Brown–Birleşik Krallık ile B.–Fransa davaları, Dutertre, 2007, s. 296 vd.).

Bu iki veri türünün istisnasının diğer veri türlerinden ayrılarak düzenlenmesinin sebebi, yalnızca ilgili kişinin hassasiyeti ve toplum içerisinde ayrımcılığa uğrama ihtimali değil; ayrıca bu verilerin çoğu zaman ilgili kişilerin yanında onun eş ve akrabalarının sağlık ve cinsel hayatına ilişkin verilerini de ortaya çıkarma ihtimalidir. Özellikle bulaşıcı ve genetik hastalıklar bakımından bir kişinin sağlığına ilişkin veri, eşi, çocuğu veya ebeveynlerinin de sağlığına ilişkin bilgi edinilmesini sağlayabilir. Örneğin HIV pozitif olan bir kişinin eşinin ya da kan transferi yaptığı bir kişinin de aynı hastalığa sahip olma ihtimali olduğundan, bu duruma ilişkin veri aslında birden fazla kişiyi ilgilendirmektedir.

Nitekim Kişisel Verileri Koruma Kurumu verdiği 09/12/2019 tarih ve 2019/372 sayılı kararında, ilgili kişinin sağlık verilerinin paylaşılması sebebiyle yakının yaptığı başvuruyu yerinde görerek veri sorumlusunu idari para cezasına mahkum etmiştir. Olayda gazete olan veri sorumlusu, şikâyet sahibinin oğluna yönelik bir köşe yazısında, "*Babasının kanser tedavisi nedeniyle bir süre önce görevine ara verdiğine"* ilişkin bir habere yer vermiştir. Şikâyetçi olan oğlu, babasının kanser hastalığının kendisinden gizlendiğini ve bu köşe yazısı üzerine öğrendiğini bunun akabinde ölüm korkusu yaşadığını ifade etmiştir. Kurum bu şikâyet üzerine, veri sorumlusunun KVKK'nın 6. maddesinde sayılan şartlardan biri olmaksızın ilgili kişinin özel nitelikli kişisel verilerinin, paylaşılmasının kanuna aykırılık teşkil ettiğini ve bu nedenle veri sorumlusu hakkında 125.000 TL idari para cezasının uygulanmasına karar vermiştir.

Kişilerin sağlıklarına ve cinsel yaşamına ilişkin veriler, yukarıdaki örnekte olduğu gibi ilgili kişiler ve hatta yakınları hakkında çok fazla bilgi içerir. Bu nedenle hem Tüzük hem de KVKK uyarınca, aydınlatılmış rıza olmaksızın işlenemez (Özer Deniz, 2022; Peto vd., 2004) Zira veri, işlemenin belirli, açık ve meşru amacı açıkça ve tereddüde yer bırakmayacak şekilde açıklanmış ve ilgili kişi buna açık rıza vermiş ise işlenebilir (Adams vd., 2004; Özer Deniz, 2022).

b. Verinin sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi

Sağlık ve cinsel hayata ilişkin verilerin sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi gerekir. Sır saklama yükümlülüğü, hukuki dayanağını öncelikle Anayasa'nın 20. maddesinden alır. Sır saklama yükümlülüğü altında olan kişilerden bahsetmeden önce sır kavramını açıklamak gerekir. Bir bilginin sır olarak kabulü için objektif ve sübjektif iki unsurun var olması aranır (Özdemir, 2010, s. 125). Sır kavramının objektif unsuru, sıra ilişkin bilginin üçüncü kişiler tarafından bilinmemesidir. Sübjektif unsuruysa, bilgiyi veren ve alanın iradesinin sır saklamaya yönelik olmasıdır. Sırlar, devlet sırrı, ticari sır, meslek sırrı gibi farklı konulara ilişkin olabilir. Konumuzu yakından ilgilendiren meslek sırrı, kişinin mesleğinin icrası vesilesiyle edindiği sırlardır. (Hakeri, 2015; Özdemir, 2010; Yılmaz, 2019). Bazı meslek gruplarına, işlerinin icrası sırasında oldukça gizli bilgilere erişebilme imkânları olduğundan, meslekleri dolayısıyla edindikleri sırları saklama yükümlülüğü getirilmiştir.

Bu yükümlülük altında bulunan meslek grupları bakımından sır saklama yükümlülüğü, meslek etiği ilkesi olmasının yanında yasal bir zorunluluktur. Dolayısıyla, bu kişiler, sır saklama yükümlülüklerini ihlal etmeleri halinde yasal yaptırımlar ile karşılaşırlar. Sağlığa ilişkin kişisel veriler bakımından sır saklama yükümlülüğü altında olan kişiler başta hekimler, İşyeri Hekimi ve Diğer Sağlık

Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmelik 11. maddesine göre iş yeri hekimleri, ebeler, hemşireler, hasta bakıcılar ve eczacılardır (Hakeri, 2015; Doğan, 2008; KVKK,2020).

Sağlık verileri en çok hasta-hekim ilişkisinde işlenmektedir. Hekimin sır saklama yükümlülüğü, Türk Borçlar Kanunu, Tıbbi Deontoloji Nizamnamesi, Hasta Hakları Yönetmeliği, Hekimlik Meslek Etiği Kuralları gibi çeşitli mevzuat hükümlerinde yer almaktadır. Hekimin sır saklama yükümlülüğü veri sorumlusu sıfatıyla KVKK hükümlerinin yanında vekilin sadakat yükümlülüğünün bir uzantısıdır. Sağlık çalışanları, mesleklerinin icrası sırasında hastalara dair hastalıkları, kalıtsal özellikleri, cinsel tercihleri, alkol, ilaç ve uyuşturucu kullanımı gibi pek çok bilgi edinirler. Mevzuat hükümleri gereğince bu şekilde edindikleri bilgileri teşhis, tedavi öncesi görüşmeler, tedavi, tedavi sonrası, hastanın ölümünden sonra sır saklama yükümlülüğü kapsamında gizli tutmaları gerekir (Hakeri, 2015, s. 891).

Kişisel Verileri Koruma Kurumu, 07/05/2020 Tarihli ve 2020/355 Sayılı kararında, veri sorumlusu olan bir eczane tarafından KVKK m. 8'de sayılan şartlar sağlanmadan ilgili kişilerin ilaç kullanımına dair verilerinin üçüncü kişiyle paylaşılmasını KVKK m. 12/4'e aykırı bulmuş ve veri sorumlusu olan eczane hakkında idari para cezası hükmedilmesine karar vermiştir (KVKK, 2018).

Uygulamada karşılaşılan bir durum ise sır saklama yükümlülüğü altında bulunmayan kişilerin de bu bilgilere erişebilmesidir. Hastane gişe çalışanları ya da teknikerlerin mesleki olarak sır saklama yükümlülüğü yoktur; ancak onlar sır saklama yükümlülüğü olan doktorların ulaşabildiği çoğu bilgiye onlar da erişebilmektedirler. Görevi gereği, sağlık veya cinsel kişisel verilere ulaşabilen bu kişiler karşısında kişisel verileri korumak adına hastane ya da doktorun gizlilik sözleşmesi yapması hem onlar hem de ilgili kişiler bakımından güvence sağlayacaktır.

Kurum'un önüne gelen bir olayda, doktor sekreteri yetkisiz olarak, e-Nabız sistemine giriş yetkisi olan doktorun yerine ilgili kişinin e-nabız sistemine girerek sağlık verilerine ulaşmıştır. Bu olayda Kurum, 21/09/2021 tarihli ve 2021/962 sayılı kararında veri sorumlusu olan doktor hakkında, kişisel veri güvenliğine ilişkin makul teknik ve idari tedbirleri almadığı için KVKK m. 12 ve 18 uyarınca idari para cezası uygulamıştır. (KVKK, 2021).

c. Veri işlemenin amacının belli olması

KVKK m. 6'da ilgili kişilerin açık rızası alınmaksızın sağlığa ve cinsel yaşama ilişkin özel nitelikli kişisel verilerin işlenebilmesi bakımından dört farklı amaç belirlemiştir. Veri işleme faaliyetinin bu istisna kapsamında olabilmesi için işleme amacının en az birinin kanunda yer alan amaçlardan olması gerekir. Sağlık verilerinin açık rıza olmadan işlenebileceği amaçlar, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi olarak dört tanedir.

Bu amaçlardan kamu sağlığı, Sağlık Bakanlığı tarafından toplum genelinde sağlık ve refah seviyesini koruma amacıyla hazırlanan yasal düzenlemeler ile korunur. Bu kapsamda, 663 sayılı Sağlık

Bakanlığı ve Bağlı Kuruluşların Teşkilatlar ve Görevleri Hakkında Kanun Hükmünde Kararname[1] ile Türkiye Halk Sağlığı Kurumu kurulmuştur. Türkiye Halk Sağlığı Kurumu, Aile Hekimliği Dairesi Başkanlığı, Toplum Sağlığı Hizmetleri ve Eğitim Dairesi Başkanlığı, Aşı ile Önlenebilir Hastalıklar Dairesi Başkanlığı, Sağlıklı Beslenme ve Hareketli Hayat Dairesi Başkanlığı, Bulaşıcı Hastalıklar Daire Başkanlığı, İzleme, Değerlendirme ve İstatistik Dairesi Başkanlığı gibi başkanlıklar olmak üzere toplam yirmi dört daire başkanlığı oluşturarak toplumun genel sağlığını korumak ve iyileştirmek amacıyla çalışır.

Kamu sağlığının korunması amacıyla kurulan kamu kurum ve kuruşlarının görev alanına salgın hastalıklar ve bunlara tedavi sağlamak ile çevre, su ve besinlerin hijyenini takip etmek, doğal afet planlarını oluşturmak, yeni sağlık politikaları belirlemek girer (Erarslan Türkmen, 2019, s. 175). Bu faaliyetler sırasında, ilgili kişilerin sağlık veya cinsel yaşamlarına ilişkin kişisel veriler, ilgili kişilerin açık rızası alınmadan işlenebilir. Örneğin, Bulaşıcı Hastalıklar Daire Başkanlığı'nın yayınladığı Bulaşıcı Hastalıklar ile Mücadele Rehberinde, bulaşıcı hastalık tanısı veya şüphesi olması halinde, ilgili kişinin hastalık bilgisi, iletişim, yaş, sağlık, konum gibi verileri işlenebilir.

İkinci amaç olan koruyucu tıp ise çeşitli tanı, bakım ve sağlık hizmetleri sunarak toplumun hastalanmadan veya salgın yaşamadan sağlığını korumayı amaçlar (Basan & Bilir, 2016, s. 44). Bu kapsamda, koruyucu sağlık hizmetlerinin asıl görevi, hastalıklar oluşmadan veya yayılmadan gerekli önlemleri almaktır (Basan & Bilir, 2016, s. 45). Bu amaçla aşılama, tütün ve uyuşturucu maddelerin kullanımının bırakılmasını veya azaltılmasını sağlama, erken teşhis amaçlı testler yapma gibi faaliyetler yapılır. Bu faaliyetlerin gerçekleşebilmesi için Sağlık Bakanlığı ve buna bağlı kurum ve kuruluşlar, ilgili kişilerin gerekli görülen sağlık verilerini açık rızası olmadan işleyebilir.

Tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi kapsamında sağlık verileri elektronik sistem üzerinden MEDULA'ya kaydedilmektedir[2]. Ayrıca, gebe ve lohusa kadınların verileri GEBLİZ sistemine[3], yenidoğan ve bebeklerin aşı kayıtları AŞI-NET'e, evlilik öncesi istenen zorunlu kan testlerinin sonuçları Kalıtsal Kan Hastalıkları Bildirimine, intihar vakaları ise Acil Servis Ünitesi İntihar Girişimi Kayıtları sistemlerine işlenmektedir.

[1] "Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname" olan KHK adı, RG, 09.07.2018 ve No: 30473 (3. mük.) yayımlanan 703 sayılı KHK.nin 25. maddesiyle "Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname" olarak değiştirilmiştir.

[2] Uygulamada, özellikle aile hekimliklerinde çalışan sağlık personeli, salt verileri sisteme girmiş olmak için verilerin elde edilmesine yönelik özel hayatın gizliliği ve mahremiyeti ihlal ederek bilgi edinmeye çalışmaktadır. Sağlık ocaklarında çalışan sağlık çalışanları, etrafta diğer hasta ve çalışanların olmasına dikkat etmeksizin, ilgili kişilerin tüm kimlik bilgilerini zikrederek, telefon üzerinden kişilerin sağlık bilgilerini öğrenmeye çalışmaktadır. Bu konuda Kurumun örnek gösterdiği kuralların, uygulamada göz ardı edildiği kanaatindeyiz.

[3] Gebliz, İstanbul İl Sağlık Müdürlüğü tarafından yürütülen ve 2008'de kurulan bir sistemdir. Sistemin toplum sağlığını koruma ve takip amacının yanında Gebliz'in neden olduğu aile içi şiddet vakaları da yaşanmıştır. Örneğin, Gebliz çalışanlarının gebe kadına haber vermeden evine gelmesi üzerine, sevgilisinden hamile kalan ve ailesine henüz gebeliği açıklamayan genç bir kızın evinde aile içi şiddet yaşanmıştır. Sistem, sonuçtan bağımsız olarak, gebelik testi yaptıran her kadını kaydetmektedir. Örnekteki gibi benzer olayların yaşanması üzerine Sağlık Bakanlığı, test yaptıran kişilere mahremiyet butonu seçeneği sunmuştur.

Dördüncü amaç ise sağlık hizmetleri ile finansmanının planlanması ve yönetiminin belirlenmesidir. Sağlık hizmetlerinin finansmanının plan ve yönetimi, toplumun tüm üyelerinin sağlık hizmetlerinden layıkıyla faydalanabilmesi amacıyla sağlık harcamalarının ve kaynaklarının belirlenmesi için gerekli iş ve işlemleri kapsar (Uğurluoğlu & Özgen, 2018, s. 1999). Bunların yanında, kaynakların verimli kullanımı ve harcamaların azaltılması için gerekli değerlendirmeler yapılır. Bu kapsamda, hasta-hastane-doktor sayı ve oranları, hastaların teşhis ve tedavi süreleri gibi veriler incelenir. Bu ve benzeri veriler, bu amaç kapsamında işlendikleri sürece ilgili kişilerin açık rızası olmaksızın ilgili kurum ve kuruluşlar tarafından işlenebilir.

d. Kişisel Verileri Koruma Kurumu tarafından belirlenen önlemlerin alınması

Özel nitelikli kişisel veriler bakımından, genel nitelikli kişisel verilerden farklı olarak Kanun işlenmesi için bir koşul daha öngörmüştür. Buna göre, özel nitelikli kişisel verilerin işlenmesi durumunda veri sorumlusunun Kişisel Verileri Koruma Kurumu'nun belirlediği yeterli önlemleri alması gerekir. Bahsi geçen bu önlemler, 31.01.2018 tarihli 30353 sayılı Resmî Gazetede yayınlanan *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"*ile ilgili KVKK kararında yer almaktadır. Kurul, bu kararında KVKK m. 6/4'teki "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır"* hükmünü esas alarak KVKK'nın 22. maddesinin (ç) ve (e) bentleri uyarınca veri sorumlularının özel nitelikli kişisel verileri işlerken alması gereken önlemleri belirlemiştir. Bu önlemler aşağıda detaylıca incelenecektir.

da. Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi

Kurumun belirlediği önlemlerin birincisi, özel nitelikli kişisel verilerin güvenliği sağlamak adına, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir politika ve prosedürün belirlenmesidir. Buna göre, özel nitelikli kişisel verileri işleyen her kurum ve kuruluşun önceden hazırlanmış, verilerin güvenliğini korumaya dair Kurumun ve Kanun'un belirlediği ilke ve kurallara uygun kuralları olmalıdır.

Bu şekilde kural belirlenirken yapılması gereken ilk şey veri sorumlusunun uhdesindeki verilerin niteliğini ve niceliğini tespit etmesidir. Veri minimalizasyonu ilkesi gereği, veri işleme amacına hizmet etmeyen veriler silinmeli, yok edilmeli ya da anonim hale getirilmelidir. Daha sonra verilerin genel ve özel nitelikli olmalarına göre uygun koruma önlemleri belirlenmelidir (Tayan, 2017, s. 47). Sağlık verilerini işleyen doktor, hastane ve benzeri sağlık kuruluşlarının her halde Kurum'un yayınladığı önlemlere tamamen uyması gerekir. Cumhurbaşkanı tarafından yayınlanan Bilgi ve İletişim Güvenliği Tedbirleri başlıklı genelgede tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren idarelerde uyulması zorunlu güvenlik tedbirleri belirlenmiştir (RG, 06.07.2019 ve No: 30823).

Kurum'un 17/03/2022 tarihli ve 2022/243 sayılı Kararına konu olayda,

"Veri sorumlusu tarafından ilgili kişinin kişisel verilerinin yer aldığı bir belgenin, aynı isme sahip başka bir kişiye gönderilmesinin; veri sorumlusu açısından sistemsel bir açığa işaret ettiği dikkate alınarak, Kurul tarafından Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğinin sağlanması hususunda

gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

b) Veri sorumlusunun bir çalışanının, talebi olmamasına rağmen müşterisinin (ilgili kişi) kişisel verilerini, kendisine yetki tanımlaması yapılan sistemler aracılığıyla kişisel amaçları için sorgulaması nedeniyle,

Kurul tarafından Kanunun 12 nci maddesinin (1) numaralı fıkrası gereğince veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari işlem tesis edilmesine karar verilmiştir." şeklinde karar almıştır (KVKK, 2020).

Kurul kararında da görüldüğü gibi sadece güvenlik politikasının belirlenmesi yeterli değildir; aynı zamanda belirlenen güvenlik politikasının uygulanabilir olması ve hatta veri sorumlusu gerektiği noktada önlem alabilir, elverişliliği ve yerindeliği kontrol edilebilir olmalıdır.

db. Kişisel verilerin işlenmesi sürecinde yer alan çalışanlara yönelik önlemler

Kurul, veri sorumlusunun veri işleme sürecinde yer alan çalışanlarına yönelik beş farklı tavsiyede bulunmuştur. Bunlar, eğitimler verilmesi, gizlilik sözleşmesi yapılması, verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması, periyodik olarak yetki kontrollerinin yapılması, görev değişikliği ya da işten ayrılanların yetkilerinin kaldırılmasıdır.

Kurul, veri sorumlularının, çalışanlarına veri güvenliği ve yasal düzenlemeler hakkında eğitim vermesini önermiştir (KVKK, 2021). Eğitimin kapsamı, yöntemi ve şekli ile ilgili bir detay düzenleme yapılmamıştır. Dolayısıyla bu konu hakkında eğitim, veri sorumlusunun kendisi, bünyesinde kurulacak bir departman ya da konunun uzmanı kimseler tarafından verilebilir.

Bu eğitimler, çalışanların işleri sırasında elde ettikleri kişisel verilerin önemini ve veri ihlalinin ilgili kişiler, veri sorumlusu ve kendileri bakımından doğurabileceği hukuki sonuçları bilmeleri bakımından önemlidir. Hastane personelinin ya da doktor sekreterinin, hasta kayıt ya da teşhis süresince edindiği bilgilerin özel nitelikli veri olarak uluslararası ve ulusal alanda korunan bir kişilik hakkı olduğunu ve bu bilgilerin özel önlemler alınarak işlenmesi gerektiğini bilmesi, kişisel sağlık verilerinin korunması konusunda alınabilecek en erken ve etkili önlemlerden biri olacaktır. Kişisel Verileri Koruma Kurumu, bu amaca uygun olarak gişe, banko ve benzeri yerlerde çalışan kişiler için bir ilke kararı vermiştir (KVKK, 2017).

Eğitim verilmesinin yanında, veri sorumlusu, çalışanları ile gizlilik sözleşmesi yaparak, işlenen verilerin, çalışma süresi içerisinde ve sonrasında, üçüncü kişiler ile paylaşmasını önleyebilir (Yılmaz, 2019; Özer Deniz, 2022). Zaman zaman, siyasi veya magazinsel olarak bilinen kişilerin sağlık sorunları veya cinsel hayatlarına ilişkin haberlerin, hastane personeli tarafından habercilerle paylaşılmasına rastlanabilmektedir. Böyle bir durumda, çalışanlar ile yapılacak bir gizlilik sözleşmesi, önleyici bir etki doğurabilir ve verilerin güvenliğini sağlayabilir.

Veri güvenliğini sağlamak adına üçüncü olarak, verilere erişim yetkisi bulunan çalışanların yetkilerinin kapsamı ve süreleri belirlenmelidir. Bu şekilde, yetki aşımının ve yetkisiz kişilerin bilgi edinmesinin önüne geçilmiş olur.

Kurum, kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında veri işlemesi hususunu değerlendirdiği olayda, *"Bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine,"* şeklinde karar vermiştir (KVKK, 2018). Kararda görüleceği üzere, teknik ve idari tedbirler almak veri sorumlusunun yükümlülüğüdür.

Tüm bunların yanında Kurum, veri sorumlusuna, yetki sahibi kişilerin yetkilerini belirlenen sınırlar içerisinde kalarak kullanıp kullanmadıklarını belirlemeye yönelik, periyodik yetki kontrol testleri yapmasını önermiştir. Bu kapsamda, görev ve yetki değişikliği yapılan ya da işten çıkarılan çalışanların yetkilerinin derhal değiştirilmesi veya sonlandırılması gerekir. Özellikle iş akdine son verilen çalışana tahsis edilen bilgisayar, şifreler veya harici belleğin geri alınması; ayrıca, kişisel verilerin kaydedildiği bir sistem varsa buna girişi sağlayan şifrenin değiştirilmesi gerekir. Kurum'a yapılan bir ihlal bildiriminde, çalışan kişi, işten ayrıldıktan sonra, sistem şifresini kullanarak eski işyerindeki verileri hukuka aykırı olarak aktarmıştır (KVKK, 2021). Bu tür olaylar bakımından şifre değişiklikleriyle, işten çıkarılan veya yetkisi sınırlandırılan kişilerin veri ihlalinin önüne geçilebilir.

dc. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamların elektronik olmasında alınacak önlemler

Kurum kişisel verilerin işlendiği ortamın elektronik olması halinde alınacak önlemi ayrıca belirterek kripto grafik yöntemlerin kullanılmasını tavsiye etmiştir. Örneğin ülkemizde, Aile Hekimliği Uygulama Yönetmeliği'nin 30. maddesi "*Kayıtlı kişi sayısı, yapılan hizmetlerin listesi, muayene edilen ve sevk edilen hasta sayısı, kodları ile birlikte konulan teşhisler, reçete içeriği, aşılama, gebe ve lohusa izlemi, bebek ve çocuk izlemi, üreme sağlığı ve bulaşıcı hastalıklar ile ilgili veriler ve Kurum tarafından belirlenen benzeri veriler evrak kayıt kriterlerine göre belirli aralıklarla düzenli olarak basılı veya elektronik ortamda Kuruma bildirilir.*" şeklindedir. Bu Yönetmelik uyarınca, her aile hekimliğine kaydedilen kişiye ilişkin veriler elektronik olarak kaydedilir. Dolayısıyla elektronik ortamda muhafaza edilen bu veriler bakımından, Kişisel Verileri Koruma Kurumu'nun belirlediği önlemlerin alınması gerekir.

Kriptoloji yönteminde bilgiler çeşitli kodlamalarla gizlenir. Düz metinler, ancak anahtar ya da şifre ile açık hale gelerek erişilebilir (Coşkun & Ülker, 2013, s. 21). Güvenliğin tam olarak sağlanması için kripto grafik anahtarların farklı ortamlarda tutulması gerekir. Bir diğer yöntem ise "*güvenli giriş katmanı*" olarak Türkçe'ye çevrilebilen, ağ üzerinden veri aktarımı sırasında sunucu ile istemci arasındaki iletişimin şifreleyen SSL (*secure socket layer*)dir. Bunun yanında, Captcha (*completely automated public turing test to tell computers and humans apart*) sistemi de kullanılmaktadır. Bu sistemde bilgisayar ile insanı ayırt edebilmek amacıyla, insanların rahatlıkla yapabileceği ancak bilgisayarların çözemeyeceği, basit sorular sorulmaktadır.

Ayrıca, elektronik sistemde gerçekleştirilen tüm işlem hareketlerinin güvenli olarak kayıt altına alınması gerekir. Bu kayıt, *log* olarak adlandırılır. Log, *"Bilişim sistemlerinin ürettiği olay kayıtlarının zaman damgalı olarak tutulması."* olarak tanımlanır. Log kayıtlarıyla, veri ekleme, düzeltme, silme gibi işlemlerinin kaydını tutularak, özellikle veri ihlali olması işleme faaliyetlerinin ne zaman ve kimin tarafından yapıldığını tespit edilebilir[4].

Bunların yanında, elektronik ortamların güvenlik güncellemelerinin, zafiyet ve sızma tarama testlerinin düzenli ve gerektiği ölçüde yapılması gerekir (KVKK, 2018). Bu kapsamda, e-devlet, UYAP, Medula, E- nabız yazılımları devletin ilgili birimleri tarafından düzenli aralıklarla kontrol edilmektedir.

Kurum, verilere uzaktan erişim sağlanabiliyorsa en az iki kademeli kimlik doğrulama sisteminin kullanılmasını tavsiye etmiştir (KVKK, 2021). İki kademeli doğrulama, yalnızca şifre kullanmanın yeterli olmadığı; şifre ile birlikte akıllı kart, telefona gelen ek şifre ya da biyometrik doğrulamanın gerektiği yöntemlerdir (Erarslan Türkmen, 2019, s. 149). Örneğin, Ulusal Yargı Ağı Bilişim Sistemi (UYAP) sistemi bir akıllı kart ve şifrenin birlikte kullanıldığı iki kademeli kimlik doğrulama sistemidir.

Son olarak, bu konuda çalışanların elektronik ortamda muhafaza edilen verilerin güvenliğine ilişkin bilgi almaları gereklidir. Bu noktada çalışanlara, korsan ve tehlikeli yazılımlarla gerçekleşecek olası bir saldırıda almaları gereken tedbirler hakkında bilgi verilmelidir. Örneğin, Kurum'un veri güvenliği rehberinde belirttiği gibi çalışanlara şirket bilgisayarları ve ağları üzerinden tehlikeli olabilecek bazı elektronik postaların açılmaması gerektiği uyarısı yapılmalıdır (Özer Deniz, 2022, s. 190).

dd. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamların fiziksel olması halinde alınacak önlemler

Özel nitelikli kişisel veriler kâğıt, ajanda ya da USB, CD ve benzeri şekilde fiziksel olarak saklanıyor ise bu verilere yetkisiz erişimin veya verilerin tahribatının önlenmesi adına Kurum tavsiye önlemler belirlemiştir. Verilere yetkisiz erişimi engellemek üzere verilerin bulunduğu ortamlara girişe ve çıkışa yetkili kişilerin belirlenmesi gerekir. Bunun için yetkili kişilerin bu ortamlara imza, kart okutma veya biyometrik yöntemler kullanarak erişebilmesi bir yöntem olabilir.

Kişisel Sağlık Verileri Hakkında Yönetmeliğin *"Genel İlke ve Esaslar"* başlıklı 5. maddesi, "*Sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirler alınır.*

(5) Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleme tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır."

[4] RG 11.04.2017 ve No: 30035'te yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliği 4. maddesinde internet toplu kullanım sağlayıcılarına ve 5. maddesinde ticari amaçla internet toplu kullanım sağlayıcılarına erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklama yükümlülüğü getirmiştir.

şeklindedir. Burada görüleceği gibi, Yönetmelik özel nitelikli olarak sayılan sağlığa ilişkin verilerin fiziksel olarak saklanması durumunda alınacak önlemleri ayrıca belirtmiştir.

Yönetmelikte yer alan önlemler çerçevesinde, bir hastanenin yapılan kan tahlili sonucunu, kapalı zarfta ilgili kişiye teslim etmelidir. Öncesinde ise tahlil sonucuna hastanedeki herkesin erişmesini önlemek adına sadece sır saklama yükümlülüğü altında bulunan veya şifre ile girilebilen bir sistemde muhafaza edilmesi gerekir.

Verilerin fiziki ortamda muhafaza edilmesi durumunda, veri sorumlusunun somut olaya uygun önlemlerin alınması, verilerin muhafaza edildiği odayı veya dolapları kilitlemesi ve anahtarları belirli ve mümkünse az kişiye zimmetlemesi gerekebilir. Verilerin arşivlendiği odanın da hırsızlık, deprem veya sele karşı korunaklı olması gerekir.

de. Özel nitelikli kişisel veriler aktarılacaksa alınacak önlemler

Özel nitelikli kişisel veriler aktarılacak ise verilerin fiziksel ya da elektronik olmasına göre farklı önlemler alınmalıdır. Elektronik ortamda muhafaza edilen veriler aktarılacak ise kayıtlı elektronik posta (KEP) hesabının kullanılması tavsiye edilir[5].

KEP hesabının önerilmesinin sebepleri, güvenilir kimlik doğrulama mekanizması sağlaması, işlemlerin kayıt altına alması ve bu kayıtların aksi ispat edilinceye kadar kesin delil sayılması olarak sayılabilir. Farklı yerlerde bulunan sunucular arasında aktarım yapılacaksa, sunucular arasında VPN kurulması veya sFTP[6] yönteminin kullanılması tavsiye edilir. Veriler fiziki olarak saklanıyorsa ve bu şekilde aktarılacaksa evrakın çalınması veya kaybolması ihtimallerine karşı gerekli önlemlerin alınması gerekir.

C. AYDINLATMA YÜKÜMLÜLÜĞÜ

1. Aydınlatma Yükümlülüğünün Kapsamı

Aydınlatma yükümlülüğü, KVKK m. 10'da "*Veri Sorumlusunun Aydınlatma Yükümlülüğü*" başlığı altında düzenlenmiştir. Bunun yanında, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de detaylı düzenlemeler yapılmıştır. Avrupa Birliği Veri Koruma Tüzüğünde ise 12. maddede, ilgili kişinin hakları başlığı altında düzenlenmiştir.

[5] Kayıtlı elektronik posta, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik "*Tanımlar ve Kısaltmalar*" başlıklı 4. maddesinde "*Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukukî delil sağlayan, elektronik postanın nitelikli şekli"* olarak tanımlanmıştır. RG, 25.08.2011 ve No: 28036.

[6] Dosya aktarım protokolü olarak adlandırılabilecek sFTP ile bir bilgisayardan bir başka bilgisayara dosya aktarımı yapılırken, o bilgisayar ile etkileşimli bağlantı kurulur. Bir dizi komut yardımıyla iki bilgisayar arasında dosya alma ve gönderme işlemleri yapılır.

Gerek KVKK m. 10 gerekse Tebliğ m. 4'e göre, veri sorumlusunun kendisi ya da yetkilendirdiği kişi, ilgili kişi ya da kişileri veri işleme faaliyetleri hakkında bilgilendirmek zorundadır (KVKK, 2020). Tebliğ'e göre, aydınlatma yükümlülüğünün yerine getirildiğini ispat yükü veri sorumlusuna aittir[7].

Aydınlatma yükümlülüğü, veri sorumlusu için kanuni bir yükümlülük olduğundan, veri işleme faaliyetinin hukuka uygun olabilmesi için veri işleme faaliyeti öncesinde açık rıza aranmayan hallerde dahi aydınlatma yükümlülüğü yerine getirilmelidir. Bu yükümlülük bakımından istisna KVKK m. 28/1 hükmüdür. Bu hükümde belirtilen durumda, veri sorumlusunun aydınlatma yükümlülüğü yoktur. Bu istisnalar, kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla bilimsel ile koruyucu ve istihbarı faaliyetler, aile fertleriyle ilgili faaliyetler kapsamında işlenmesi, planlama ve istatistik gibi amaçlarla işlenmesi veya yargı makamları veya infaz mercileri tarafından işlenmesidir.

Aydınlatma yükümlülüğünün içeriği, asgari olarak, kanun maddesinde belirtilmiştir. Maddeye göre veri sorumlusu, kendi ve varsa temsilcinin kimliği, ilgili kişinin kişisel verilerinin hangi amaçları elde etmek için işleneceği, işlenen bu verilerin kimlere ve hangi amaçlarla aktarılabileceği, kişisel verilerin elde edilme yöntemleri ve bunun hukuki sebepleri ile KVKK m. 11'de yer alan ilgili kişinin hakları konusunda bilgi vermek zorundadır. Maddede belirtilen bilgilerden daha fazla bilgi verilmesi de mümkündür. Örneğin, aktarım yapılacaksa aktarma yöntemleri hakkında detaylı bilgiler de verilebilir. Tabi ki verilecek bilgilerin, ilgili kişinin kafasını karıştırmaması ve anlaşılması kolay olması gerektiğine dikkat edilmelidir.

Maddede yer alan hususların yanında, veri sorumlusunun Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) bildirdiği hususların da aydınlatma metninde yer alması gerekir. Bir başka deyişle, VERBİS'e yapılan bildirim ile aydınlatma metnin içeriğinin birbirine uyumlu olması gerekir. Örneğin, bir tıp merkezi, VERBİS'e kayıt esnasında sağlık verilerinin sadece ilgili kamu kurum ve kuruluşlarına aktarılacağı yönünde bir bildirim yapmış iken hastalara sunduğu aydınlatma metninde sağlık verilerinin başka bir veri sorumlusuna aktarılmayacağı şeklinde bilgi yer almamalıdır. İlgili kişilere, VERBİS'e kayıt

[7] Hasta-doktor ilişkisi, aynı zamanda bir tüketici işlemidir. Hasta, ilgili kişinin KVKK kapsamında sahip olduğu hakların yanında Tüketicinin Korunması Hakkında Kanun (TKHK) kapsamında da bir takım haklara sahiptir. Bu haklardan birisi de bilgilendirilme hakkıdır. Bu bilgilendirme hakkı, tüketici ile hizmet sağlayıcısı arasında kurulan sözleşme hakkında bilgi verilmesini kapsamakla birlikte verilerin işlenmesi hakkında bilgi verilmesini de kapsar. Tüketici işlemi olmasının bir diğer yönü ise haksız şartlar bakımından olacaktır. Tüketici olan hasta (ilgili kişi), ile yapılan sözleşmelerde haksız şart olarak düzenlenen bir madde tüketici bakımından geçerli olmayacaktır. KVKK ile TKHK, aydınlatma yükümlülüğü bakımından birlikte değerlendirildiğinde, veri sorumlusu olan (hizmet sağlayıcısı) doktor ya da hastanenin, aydınlatma yükümlülüğünü kendi lehine ve tüketici aleyhine olacak şekilde sınırlandırması veya ortadan kaldırması geçerli olmayacaktır. Örneğin, hasta (ilgili kişi) ile veri sorumlusu (hizmet sağlayıcısı) doktor ya da hastane ile yapılan sözleşmede, aydınlatma yükümlülüğünün yapıldığının ispatının ilgili kişiye yükleyen veya verilerin güvenliğinden veri sorumlusunun sorumlu olmadığı belirten bir sözleşme maddesi ilgili kişi hasta bakımından hüküm ve sonuç doğurmayacaktır. Zira bu yönde bir düzenleme KVKK'ya aykırı olduğu gibi bir de tüketici bakımından haksız şarttır. (Aydoğdu & Kahveci, 2021, s. 97 vd.)

yapıldığı şekilde, ilgili kamu kurum ve kuruluşlarına aktarılacağı bilgisinin açık rızalarının alınmasından önce verilmesi gerekir.

İşleme faaliyetinin belli, açık ve meşru bir şekilde belirtildikten sonra ilgili kişiye aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılacağı alıcı grupları ve neden bu alıcı gruplarına aktarımın yapılacağının belirtilmesi gerekir. Veri sorumlusunun, uhdesindeki verileri kiminle ve neden paylaşacağını bilmek ilgili kişinin KVKK m. 11 kapsamındaki haklarından biridir. Veri sorumlusunun aydınlatma yükümlülüğü, ilgili kişinin bu madde kapsamındaki haklarının kullanımı için de gereklidir.

Tebliğe göre, aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir. Zira bu şekilde ilgili kişi, yanlış anladığı ya da kendisine eksik ifade edilen bilgilere göre açık rıza göstermiş olur. İlgili kişi, kendisine doğru şekilde bilgi verilse rıza göstermeyeceği bir işleme faaliyetine, yanlış bilgilere dayanarak rıza verebilir. Bu da kişinin iradesini etkileyebilir. Örneğin, hastaya verilerinin yalnızca Sağlık Bakanlığı'na aktarılacağı belirtilmesine rağmen veriler Ar-Ge çalışmaları için ilaç şirketleriyle paylaşılıyorsa, bu bilgilendirme yanlış olacaktır.

Kişisel verileri işleme amacı, aydınlatma yükümlülüğü yapıldıktan ve açık rıza beyanı alındıktan sonra değişir ya da yeni bir amaç eklenirse, veri sorumlusunun ilgili kişiyi bu değişiklik veya yeni amaç ile ilgili tekrar bilgilendirmesi gerekir (Dülger, 2019; Özer Deniz, 2022). İşleme faaliyetinin hukuka uygun olarak devam edebilmesi için bu bilgilendirme sonrası ilgili kişi bu değişiklik veya eklenen amaca tekrar açık rıza göstermelidir.

Bilgilendirmenin amacına ulaşabilmesi için ilgili kişinin anlayabileceği şekilde yapılması gerekir (Avcı Braun, 2018; Dülger, 2019; Özer Deniz, 2022). Dolayısıyla bilgilendirmenin içeriği ve kullanılan dil önemlidir. İlgili kişi, okuduğunda anlayamayacağı teknik terimler içeren, çok uzun ve karmaşık, muğlak ifadeler içeren bir aydınlatma metni imzaladığında bilgilendirme yükümlülüğünün yerine getirildiği söylenemez (Custers vd., 2013; Özer Deniz, 2022).

Kurum'un önüne gelen olayda veri sorumlusu aydınlatma metni olarak hazırladığı metinde kişisel veri kategorilerini sıralayıp, "bunlarla sınırlı olmaksızın" şeklinde bir ifadeye yer vermiştir. Ayrıca, veri sorumlusu olarak kendisinin, hangi amaçlarla veri işleyeceğini belirtmeksizin sadece çeşitli veri işleme amaçlarını eklemiş ve uygun gördüğü üçüncü kişilerle ve/veya yurt dışında paylaşılabileceğini belirtmiştir. Kurum, 20/05/2020 tarihli ve 2020/404 sayılı kararında, bu metnin aydınlatma metni olarak kabul edilemeyeceğine zira muğlak ve belirsiz ifadelerin bulunduğuna ve veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediğine karar vermiştir (KVKK, 2020).

Konovalova v. Rusya davasında hastane, aydınlatma metninde, sayı veya cinsiyet gibi detaylara yer vermeksizin, "*Hastanemizde tedavilerin jinekoloji çalışan öğrencilerin eşliğinde yapılmasına saygı göstermenizi rica ederiz. Bu sebeple, tüm hastalar öğrenme sürecinin bir parçasıdır"* şeklinde bir ifadeyle, tıp öğrencilerinin hastaların muayenesi sırasında doktorların yanında olabileceklerini belirtir. Daha sonra başvurucu hasta, oldukça kalabalık bir öğrenci grubu eşliğinde doğum yapmak zorunda kalınca, özel hayatının ihlal edildiği bahsiyle hastane aleyhine dava açar. Hastane ise bu konuda hastaya bilgi verildiğini ileri sürer. AİHM, hastanenin bilgilendirme sırasında tıp öğrencilerinin müdahaleye katılımının kapsamını ve süresini belirtilmediğini, bilgilendirmenin açık yapılmadığını, hastanın doğum yaptığı sırada tıp

fakültesi öğrencilerinin odada bulunmasının kişilik hakkı ihlali olduğunu belirterek başvurucu hastayı haklı bulur (The Council of Europe, 2018).

Aydınlatma metninin kapsamı bakımından ayrıca, sağlık alanındaki teşhis ve tedaviler sırasında ortaya çıkan tesadüfi sonuçlar hakkında bilgilendirme yapılmasının gerekliliği tartışılmalıdır. Esasında tartışmalı olan nokta, ilgili kişinin tesadüfi teşhis ve tedavi sonuçlarının üçüncü bir kişiyi ilgilendirmesi durumudur. Tesadüfi sonuçlar yalnızca ilgili kişiyi ilgilendirebileceği gibi üçüncü kişileri de ilgilendirebilir. Bu durumda, iki ihtimalin de değerlendirilmesi gerekir.

Bu değerlendirme yapılırken, aydınlatma beyanı esas alınmalı ya da hastaya bu konuyla ilgili tercihi önceden sorulmalıdır. (Doğan, 2008; Stumper, 1996). Hasta Hakları Yönetmeliği m. 20'de, *"İlgili mevzuat hükümleri ve/veya yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında; kişi, sağlık durumu hakkında kendisinin, yakınlarının ya da hiç kimsenin bilgilendirilmemesini talep edebilir."* şeklinde düzenleme yer almaktadır. Dolayısıyla, aydınlatma yükümlülüğü yerine getirilirken, tesadüfi olarak ortaya çıkan sonuçların akıbetine ilişkin bilgi verilmelidir. Böylece, ilgili kişi olan hasta, bu sonuçların paylaşılmasına ya da paylaşılmamasına yönelik rıza beyanını geçerli olarak kullanabilir.

2. Aydınlatma Yükümlülüğünün Şekli

Aydınlatmanın ne şekilde yapılacağı ile ilgili tek bir kural yoktur. Tebliğ'de veri sorumlusu ya da yetkilendirdiği kişinin sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılarak aydınlatma yükümlülüğünü yerine getirmesi gerektiği düzenlenmiştir. Bilgilendirme, sade ve okunabilir bir metin ile veya sözlü olarak yapılmalıdır (Ayözger Öngün, 2019; Küzeci, 2020). Somut olaya en uygun, ilgili kişinin en kolay ve rahat ulaşabileceği aydınlatma şekli seçilmelidir. Bu çerçevede, yüz yüze ya da uzaktan iletişim araçları, kısa mesaj, elektronik posta ile ya da panoya asılacak şekilde bildirim yapılabilir.

Tebliğ m. 5'te açıkça belirtildiği gibi, açık rızanın gerektiği hallerde, açık rıza ve aydınlatma metni mutlaka ayrı ayrı olmalıdır. Aynı metin içerisinde hem aydınlatma hem de açık rıza alınmaması gerekmektedir (KVKK, 2020).

Aydınlatma yükümlülüğü *katmanlı* olarak yapılabilir. Katmanlı bildirimden kastedilen, ilgili kişinin, kanuni olarak yapılması gereken asgari bilgilendirme yapıldıktan sonra daha fazla ve detaylı bilgilere ulaşmak istemesi halinde, başka bir ortama yönlendirilmesidir (KVKK, 2018). Örneğin, telefon konuşması başlangıcında "*Görüşmeler kalite ve hizmet standartları gereği kayıt altına alınacaktır. Detaylı bilgi için 0'ı tuşlayın.*" şeklinde yapılan bir aydınlatma, katmanlı aydınlatmadır. Bu şekilde yapılan katmanlı bildirimin geçerli olması için ilgili kişinin detaylı bilgiye erişiminin derhal mümkün olması gerekir (KVKK, 2021).

Uygulamada çoğu çağrı merkezi, görüşmelerin kayıt altına alınacağını ifade ettikten sonra detaylı bilgi için internet sitesine yönlendirmektedir. Ne var ki, bu bir katmanlı aydınlatma olmayacaktır (KVKK, 2022). Zira bu durumda ilgili kişinin görüşmeyi sonlandırıp imkânı varsa belirtilen internet sitesini ziyaret edip sonra görüşmeye devam etmesi gerekecektir. Oysaki olması gereken, kişinin görüşmelere devam etmeden önce ancak başka bir iletişim kanalı gerekmeksizin detaylı bilgiye erişebilmesidir

(KVKK, 2021). Dolayısıyla, çağrı merkezleri bakımından geçerli bir katmanlı aydınlatma beyanı, ilgili kişinin görüşmeyi sonlandırmadan ancak başka bir tuşa basarak bir başka konuşmaya yönlendirilmesi olmalıdır.

3. Aydınlatma Yükümlülüğünün Yapılacağı Zaman

Tebliğ m. 5'e göre, kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir. Açık rızanın geçerli olabilmesi için ise bu yükümlülüğün rıza beyanı verilmeden önce gerçekleşmiş olması gerekir. Dolayısıyla, veri sorumlusu, veri işleme faaliyeti öncesinde ilgili kişiden açık rıza almadan önce ilgili kişiyi aydınlatmış olmalıdır (Custers vd., 2013, s. 446). Bilgilendirmenin veri işleme faaliyetinden sonra yapılması, ilgili kişinin bilgilendirildiği anlamına gelmeyecektir (Avcı Braun, 2018, s. 15; Erarslan Türkmen, 2019). Bunun yanında, veri işleme amacının değişmesi veya yeni bir işleme amacı eklenmesi halinde de bu değişiklik öncesi aydınlatma yükümlülüğü tekrar yapılmalıdır.

Kişisel verilerin ilgili kişi dışında bir kaynaktan elde edilmesi hali Tebliğ m. 6'da düzenlenmiştir. Madde, "*Kişisel verilerin ilgili kişiden elde edilmemesi halinde; kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir."* şeklindedir.

Buradaki makul sürenin ne kadar olduğu belirsizdir. Somut olaya göre, uygun bir süre olmalıdır. Ne var ki, aşağıda belirtileceği gibi, aydınlatma yükümlülüğünün yerine getirilmemesinin hukuki sonucu, veri sorumlusuna idari para cezası hükmedilmesidir. Dolayısıyla, "*makul süre*" gibi belirsiz bir ifadenin bu kapsamda kanunilik ilkesine aykırı olduğu düşünülebilir (Karunçu, 2019, s. 41).

D. AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMEMESİNİN HUKUKİ SONUÇLARI

KVKK'nun "Suçlar ve Kabahatler" başlıklı beşinci bölümünde aydınlatma yükümlülüğünün yerine getirilmemesinin hukuki sonucu düzenlenmiştir. KVKK m. 18/1-a'ya göre aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk Lirası'ndan 100.000 Türk Lirası'na kadar idari para cezasına hükmedilir (KVKK, 2018). Bu para cezası, gerçek kişiler ile özel hukuk tüzel kişisi olan veri sorumlusu hakkında uygulanır. Aydınlatma yükümlülüğü ihlali, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde gerçekleşir ise, ihlalin gerçekleştiği kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri hakkında disiplin hükümlerine göre işlem yapılacağı düzenlenmiştir. Kurul, aydınlatma metni ile açık rıza beyanını aynı metin içerisinde düzenlemesinden dolayı aydınlatma yükümlülüğünü yerine getirmeyen veri sorumlusuna 50.000 TL idari para cezası vermiştir (KVKK, 2020).

Kurum, hakkaniyeti sağlama amacıyla, idari para cezasının miktar aralığını oldukça geniş tutmuştur. Kanun gerekçesinde, farklı ekonomik güçlerdeki veri sorumluları arasında hakkaniyet açısından denge kurmak amacıyla bu şekilde geniş bir aralık olduğu belirtilmiştir (KVKK, 2020). Kurul'un kararlarına karşı yargı yolu açıktır. Kurul'un idari para cezalarına karşı tebliğ veya tefhimden itibaren on beş gün içerisinde-n sulh ceza hâkimliğine başvurulabilir.

Sonuç

Kişisel sağlık verileri, KVKK m. 6 kapsamında özel nitelikli kişisel veri olarak kabul edilmiştir. KVKK uyarınca özel nitelikli kişisel veriler, ilgili kişinin açık rızası olmaksızın işlenemez. Geçerli bir rıza beyanı için ilgili kişinin rıza göstermeden önce aydınlatılmış olması gerekir. Böylece ilgili kişi, hangi verilerinin ne amaçla işleneceği bilgisini edinir ve bu şekilde işleme faaliyetine rıza gösterir. Aydınlatma yükümlülüğü, hem KVKK m. 10 hem de Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de veri sorumlusuna yüklenmiştir. Tebliğ'de aydınlatmanın yapılmasına ilişkin detaylı düzenlemeler yer almaktadır. Bunun yanı sıra, KVKK m. 6/3'te açık rıza olmaksızın kişisel sağlık verilerinin işlenebileceği istisna durumlar düzenlenmiştir. Bu hallerde açık rıza olmaksızın ilgili kişinin sağlık verisi işlenebilir.

Aydınlatma yükümlüğü KVKK m. 10 ve Tebliğ uyarınca, ilgili kişileri veri işleme faaliyetleri hakkında bilgilendirmelidir. Bu bilgilendirme, veri sorumluluğunun kanuni yükümlülüğü olmasının yanında ilgili kişinin haklarını kullanabilmesi adına da önemlidir. Aydınlatma yükümlülüğünde yer alan bilgilerin, VERBİS'e kayıt sırasındaki bilgiler ile paralel olması ve amacın değişmesi halinde yinelenmesi gerekir. Aydınlatma beyanına ilişkin şekil Tebliğ'de düzenlenmiştir. Bunun yanında, kullanılan dil ve ifadelerin net ve anlaşılır olması da oldukça önemlidir. Aydınlatma yükümlülüğünün yerine getirilmemesi KVKK'da kabahat olarak düzenlendiğinden, ihlali halinde veri sorumlusu aleyhine idari para cezası hükmedilmesi gündeme gelecektir.

Etik Kurul İzni

Bu çalışma etik kurul izni gerektiren bir çalışma grubunda yer almamaktadır.

Kaynakça

Abik, Y. (2018). Kişisel sağlık verilerinin medeni hukuk bakımından korunması. Hakeri & Doğan (Eds.). *II. Uluslararası Tıp Hukuku Kongresi Bildirileri Kitabı*, 537-613.

Adams, T., Budden, M., Hoare C., & Sanderson H. (2004). Lessons from the central hampshire electronic health record pilot project: Issues of data protection and consent. *British Medical Journal, 328*(7444), 871- 874.

Aldaş, C. N. (2018). Elektronik sağlık kayıtları ve dijital hastane kavramları, *Kişisel Sağlık Verileri Kongresi,* 112-115. İstanbul Türk Tabipleri Birliği Yayınları.

Aşıkoğlu, İ. Ş. (2018). *Avrupa Birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri.* XII Levha Yayınları.

Avcı Braun, C. (2018). Kişisel verilerin işlenmesinde rıza. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, *15*(1), 13-35.

Aydoğdu, M., & Kahveci N. (2021). *Tüketici hukuku.* Adalet Yayınevi.

Ayözger Öngün, Ç. (2019). *Kişisel verilerin korunması hukuku.* Beta Yayınları.

Basan, N. M., & Bilir, N. (2016). Koruyucu sağlık hizmetlerinde önleme çelişkisi ve nedenleri. *TAF-PMB, 15*(1), 44-50.

Coşkun, A., & Ülker, Ü. (2013). Ulusal bilgi güvenliğine yönelik bir kriptografi algoritması geliştirilmesi ve harf frekans analizine karşı güvenirlik tespiti. *Bilişim Teknolojileri Dergisi*, *6*(2), 21-32.

Custers, B.,Van Der Holf, S., Schermer, B., & Appleby Arnold, S. (2013). Informed consent in social media use- the gap between user expectations and EU personal data protection law. *Scripted*, *10*(4), 437-443.

Develioğlu, H. M. (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*. XII Levha Yayınları.

Doğan, C. (2008). Sağlık haklarından hekimlerin sır (kişisel veri) saklama mükellefiyeti. *Ankara Barosu I. Sağlık Kurultayı, 1-3 Kasım,* 105-144.

Dülger, M. V. (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, *1*(2), 43-80.

Dülger, M. V. (2019). *Kişisel verilerin korunması hukuku.* Hukuk Akademisi.

Erarslan Türkmen, S. (2019). *Özel nitelikli kişisel verilerin işlenmesinde açık rızanın aranmadığı haller.* XII Levha Yayınları

Ferretti, F. (2012). A European perspective on data processing consent through the re-conceptualization of european data protection's looking glass after the Lisbon treaty: Taking rights seriously. *EDPL*, (2), 473–506.

Forbes, (2012, Şubat 16). https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=6def7ceb6668.

Fry, T. F. (1983). *Data processing.* Butterworths .

Gilles, D. (2007). *Extraits clés de jurisprudence – cour européenne des Droits de l'Homme, çev. Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler*. Avrupa Konseyi Yayınları.

Hakeri, H. (2022). *Tıp hukuku.* Seçkin Yayınları.

Julian P., Fletcher O., & Gilham, C. (2004). Data protection, ınformed consent and research. *British Medical Journal, 328*(7447), 1029-1030.

Karunçu, S. (2019). *Kişisel verilerin korunması kanunu kapsamında aydınlatma yükümlülüğünün yerine getirilmemesi kabahati* (Yayımlanmamış yüksek lisans tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Kişisel Verileri Koruma Kurumu (2022). https://www.kvkk.gov.tr/Icerik/5461/2019/122.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6956/2020-769.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6914/2020-407.

Kişisel Verileri Koruma Kurumu (2022). https://www.kvkk.gov.tr/Icerik/5364/2018-143.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6968/2021-407.

Kişisel Verileri Koruma Kurumu (2022). https://www.kvkk.gov.tr/Icerik/4114/2017-62.

Kişisel Verileri Koruma Kurumu (2022). https://www.kvkk.gov.tr/Icerik/5248/2018-63.

Kişisel Verileri Koruma Kurumu (2022). Kamuoyu duyurusu (Veri ihlali bildirimi), https://www.kvkk.gov.tr/Icerik/6754/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Sezgi-Dental-Agiz-ve-Dis-Sagligi-Polikliniği.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6965/2021-140.

Kişisel Verileri Koruma Kurumu (2022). Kişisel veri güvenliği rehberi (Teknik ve idari tedbirler), https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

Kişisel Verileri Koruma Kurumu (2022). https://www.kvkk.gov.tr/Icerik/6874/2020-71 .

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6913/2020-404.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/5420/2018-90.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/7104/magazalarda-alısverıs-sırasında-ılgılı-kısılere-sms-ıle-dogrulama-kodu-gonderılmesı-suretıyle-kısısel-verılerın-ıslenmesıne-ılıskın-kamuoyu-duyurusu.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/SharedFolderServer/CMSFiles/28d8adba-2b41-41b2-bf36-d0ff0d845666.pdf.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/7112/2021-85

Kişisel Verileri Koruma Kurumu (2022). 6698 sayılı kişisel verilerin korunması kanunu kapsamında idari para cezası tutarları, https://kvkk.gov.tr/Icerik/7181/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Idari-Para-Cezasi-Tutarlari.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6913/2020-404.

Kişisel Verileri Koruma Kurumu (2022). https://kvkk.gov.tr/Icerik/6993/2021-407.

Küzeci, E. (2018). Sağlık bilişim teknolojileri ve yeni hukuksal soru(n)lar. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, *9*(1), 477-506.

Küzeci, E. (2020). *Kişisel verilerin korunması.* Yetkin Yayınevi.

Oğuzman, M. K., Seliçi, Ö., & Oktay Özdemir, S. (2021). *Kişiler hukuku.* Filiz Kitapevi.

Orak, B. (2019). *Kişisel sağlık verilerinin korunması.* Yetkin Yayınları.

Özer Deniz, M. (2022). *Özel nitelikli kişisel verilerin işlenmesi ve bundan doğan sorumluluk.* XII Levha Yayınları.

Özdemir, H. (2010). Hadım etme ve hekimin sır saklama yükümlülüğü. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 14*, 125-164.

Polat, A. (2019). *Sorumluluk hukukunda rıza*. XII Levha Yayınları.

Somer, P. (2011). Tıbbi kayıtlar. *Ankara Barosu Yayınları*, 526-554.

Stumper, K. (1996). *Informationelle selbstbestimmung und DNA-analysen: zur zulässigkeit der DNA.* Peter Lang GmbH.

Sütçü, S., & Tosyalı, H. (2016). Klinik karar destek sistemleri. İçinde B. Mendi (Ed.), *Sağlık bilişimi ve güncel uygulamalar* (ss. 99-110). Nobel Yayınları.

Taşatan, C. (2017). *Hekimin kayıt tutma yükümlülüğü kapsamında tıbbi kayıtlar.* XII Levha Yayınları.

Tayan, O. (2017). Concepts and tools for protecting sensitive data in the IT industry: A review of trends, challenges and mechanisms for data-protection. *International Journal of Advanced Computer Science and Applications, 8*(2), 46-52.

The Council of Europe, No. 37873/04, http://www.echr.coe.int.

Uğurluoğlu, E., & Özgen, H. (2008). Sağlık hizmetleri finansmanı ve hakkaniyet. *Hacettepe Sağlık İdaresi Dergisi, 11*(2), 1999-2026.

Yılmaz, S. S. (2019). *Tıp alanında kişisel verilerin açıklanması suçu*. Seçkin Yayınları.