



BIYOMETRİK VERİLERİN İŞLENMESİNDE DİKKAT EDİLMESİ GEREKEN HUSUSLARA İLİŞKİN REHBER

GİRİŞ

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla Türkiye Büyük Millet Meclisi tarafından 24.03.2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun), 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

Kanunun “*Özel nitelikli kişisel verilerin işlenme şartları*” başlıklı 6 ncı maddesinde “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 veriler olarak sayılmıştır.

Kanun ile özel nitelikli kişisel veriler arasında sayılan biyometrik veri, bugüne kadar yayımlanmış mevzuatta kapsamlı olarak tanımlanmamıştır. Bununla birlikte, kişisel verilerin korunması alanında önemli değişiklikler yapan ve yenilikler getiren Avrupa Birliği Genel Veri Koruma Tüzüğü’nün (GVKT) 4 üncü maddesindeki biyometrik veri tanımının bu alanda şimdiye kadar yapılmış en kapsayıcı tanım olduğu düşünülmektedir. Bu tanıma göre biyometrik veri; “*yüz görüntüleri veya daktiloskopi¹ veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik² veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir.*” şeklinde tanımlamıştır. GVKT’nin tanımında da yer aldığı üzere, kişisel verilerin biyometrik veri niteliğini haiz olabilmesi için;

1Daktiloskopi: Parmak izine dayanarak kimlik belirleme yöntemi (<https://sozluk.gov.tr/>)

2Fizyolojik: Fizyoloji ile ilgili, vücutla ilgili, (<https://sozluk.gov.tr/>)

- Kişinin fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özellikleri veri işleme sonucunda ortaya çıkarılmalı,
- Ortaya çıkarılan özellikler kişinin kimliğini tanımlamaya yarayan ya da kişinin kimliğini doğrulayan kişisel veriler olmalıdır.

Kanunun kabulü öncesinde bazı yargı kararlarında da biyometrik yöntemlere ilişkin tanımlamaların yer almış olduğu görülmektedir. Örnek olarak; *“Biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilmek suretiyle, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğu”*³⁴ , şeklindeki tanım gösterilebilir.

Bu tanımlardan hareketle “biyometri” ile insana ait fiziksel veya davranışsal özellikler ifade edilmekte olup, biyometrik veriler kişiye özgü, benzersiz ve tektir. Biyometrik veriler, kişilerin unutmamasının mümkün olmadığı, genelde ömür boyu değişmeyen ve herhangi bir müdahaleye gerek olmaksızın zahmetsiz bir şekilde sahip olunan verilerdir⁵. Biyometrik verilerin kullanılması sayesinde kişilerin birbirlerinden ayırt edilmeleri çok kolay bir hale gelmekte ve birbirleriyle karıştırılma ihtimalleri neredeyse ortadan kalkmaktadır.

Kişinin parmak izi, retinası, avuç içi, yüzü, el şekli, irisi gibi biyometrik verileri fizyolojik nitelikli biyometrik verileri oluşturmakta iken; kişinin yürüyüş biçimi, klavyeye basış biçimi, araba sürüş biçimi gibi biyometrik verileri ise davranışsal nitelikli biyometrik verileri oluşturmaktadır. Fizyolojik nitelikli biyometrik veriler,

3 Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararı

4 Danıştay'ın tanımına ek olarak belirtmekte fayda görülmektedir ki, yüz geometrisi de el geometrisi gibi işlem görmektedir.

5 Satapathy S. C. & Joshi A. (2017). Information and Communication Technology for Intelligent Systems (ICTS 2017), Bhatnagar S. Cooperative Multimodal Approach for Identification – (Volume 1, s. 13-18)

genellikle değişmeyen ve parmak izi, retina, iris gibi vücudumuzda taşıdığımız özelliklerin bütünüdür. Davranışsal biyometrik veriler ise yürüyüş biçimi, akıllı telefon ve benzer cihazları kullanırken ekranı kaydırmak için sergilenen hareketler, klavyeye basış biçimi, araba sürüş biçimi gibi davranışsal özelliklerdir.

Biyometrik verilerin işlenmesinde, biyometrik veri işleme şartlarının mevcudiyeti ve Kanunun 4 üncü maddesinde düzenlenen genel ilkelere riayet edilmesi önem arz etmektedir. Kanunun 6 ncı maddesinin üçüncü fıkrasına göre, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Bu çerçevede, biyometrik veriler açık rıza yoksa kanunlarda öngörülen hallerde işlenecektir. Anılan Kanun hükmünden de anlaşılacağı üzere, başka kanunlarda biyometrik verilerin işlenmesine dair hükümlerin açıkça yer alması durumunda ilgili kanunlarda yer alan hükümler uygulanacaktır. Örneğin, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67 nci maddesinde yer alan sağlık hizmetlerinden yararlanmak amacıyla biyometrik verinin alınmasına ilişkin düzenleme ve 5490 sayılı Nüfus Hizmetleri Kanununun 7 nci maddesinde yer alan, aile kütüklerinde biyometrik veri bilgisinin de bulunduğu düzenlemeleri kanunlarda öngörülen hâllere örnek teşkil etmektedir. Diğer bir deyişle, biyometrik veri işlemenin kanunlarda öngörülmesi durumunda, söz konusu hükmün şüpheye yer bırakmayacak kadar açık olması gerektiği değerlendirilmektedir.

Ayrıca, biyometrik verilerin işlenmesinde **her zaman Kanunun 4 üncü maddesinde düzenlenen genel ilkelere uyulması gerekmektedir.** Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hüküm altına alınmıştır.

Bununla birlikte, 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 düzenleme altına alınmıştır.

Biyometrik verilerin hukuka uygun olarak işlenip işlenmediği hususunda Kanunda öngörülen şartların mevcudiyetinin yanısıra somut olay çerçevesinde yorum yapılması da önem arz etmektedir. Nitekim Kurumumuz internet sitesinde yayımlanan “Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/81 sayılı Kararı ve 31/05/2019 tarihli ve 2019/165 sayılı Karar Özeti”nde açık rıza ve ölçülülük hususuna ilişkin değerlendirmeler yer almaktadır. Belirtmek gerekir ki, somut olayın gerektirdiği durumlar ve Kanuna uygun olduğu ölçüde Kurul farklı durumlarda farklı kararlar da verebilecektir.

Biyometrik veri işleme hususlarının açıklığa kavuşturulabilmesi için Kanunun 6 ncı maddesinde özel nitelikli kişisel veri olarak sayılan biyometrik veri işlenmesinde göz önünde bulundurulması gereken hususlara ilişkin olarak bu Rehber İlke Kararı hazırlanmıştır.

BIYOMETRİK VERİ İŞLEME İLKELERİ

1. Veri sorumlusu, Kanunun 4 üncü maddesinde yer alan genel ilkelere ve 6 ncı maddesinde düzenlenen şartlara uygun bir şekilde, ancak aşağıda yer alan ilkeler doğrultusunda biyometrik verileri işleyebilecektir.
- a) Temel hak ve özgürlüklerin özüne dokunmaması: Kişisel verilerin korunması hakkı, Türkiye Cumhuriyeti Anayasası'nda (Anayasa) düzenlenen temel hak ve özgürlüklerden biri olması sebebiyle, biyometrik veri işleme faaliyetlerinin de Anayasa'da öngörülen temel hak ve özgürlükler bakımından temel güvencelere tabi olması gerektiği açıktır ve bu noktada ölçülülük hususu büyük önem arz etmektedir.
- b) Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması: Bu ilke ile veri sorumlusunun ulaşmak istediği amaç bakımından başvuracağı yöntemin elverişli olması hususu ifade edilmektedir. Anayasa Mahkemesi'nin 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararında elverişlilik, *"getirilen kuralın ulaşılmak istenen amaç için elverişli olması"* şeklinde tanımlanmıştır. Biyometrik veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması gerekmekte olup, aracın yardımıyla istenilen neticeye yaklaşılabilirse, o aracın elverişli olduğu kabul edilebilecektir⁶.
- c) Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması: Anayasa Mahkemesi'nin 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararında vurgulandığı üzere; *"(...) "gereklilik" getirilen kuralın ulaşılmak istenen amaç bakımından gerekli olmasını (...) ifade eder."* Gereklilik ilkesi, aynı amacın gerçekleşmesine olanak tanıyan birden fazla aracın olması durumunda bunlar arasından en az müdahaleci olan aracın seçilmesidir⁷.

6 Metin, Yüksel, (2017) Temel Hakların Sınırlandırılması ve Ölçülülük. SDÜHFD, Cilt:7, Sayı:1, s. 8-9

7 Metin, Y. s.11

Daha az sınırlayıcı bir müdahale ile aynı veya daha iyi bir sonuç elde edilebilecek ise, bu kapsamda kullanılan araç gereklilik ilkesine aykırı olacaktır⁸. Diğer bir deyişle, biyometrik veri işlemenin yerine herhangi bir alternatifin mevcut olması durumunda biyometrik verinin işlenmesi gerekli olmayacağından söz konusu veriler işlenemeyecektir. Bu husus, Kişisel Verileri Koruma Kurulu'nun (Kurul) 25/03/2019 tarihli ve 2019/81 sayılı Kararı ve 31/05/2019 tarihli ve 2019/165 sayılı Kararı ile "(...) Spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken kişilerin biyometrik veri niteliğindeki avuç içi izi verisinin alınmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin (2) numaralı fıkrasında yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile bağdaşmadığı (...)" şeklinde ifade edilmiştir. Anılan Kurul Kararında da belirtildiği üzere, herhangi bir alternatifin bulunması durumunda biyometrik verinin işlenmesi ölçülü olmayacaktır.

Bu kapsamda alternatifin bulunması durumunu iki örnekle açıklamak gerekirse; örneğin, Kurulun da vermiş olduğu Karar'da spor salonunun giriş çıkışlarda biyometrik veri almak yerine daha farklı araçlarla aynı amaca yönelik bir sistem kullanabileceği öngörülmekteyken bir başka örnekte, yüksek güvenlik düzeyi gerektiren Nükleer Santral giriş çıkışı için daha elverişli ve gerekli bir yöntem olan biyometrik sistemler kullanılabilir. Bu bariz olan iki örnek dışında her somut olayda amaca bakarak yorum getirilmeli, biyometrik veri işleyen veri sorumlusu veriyi neden işlediğini açıkça belirtmeli ve işlemek zorunda olduğunu kanıtlamalıdır.

- ç) Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması: Anayasa Mahkemesi'nin 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararında orantılılık "*getirilen kural ile ulaşılmak istenen amaç arasında olması*

8 Metin, Y. s.11

gereken ölçü”şeklindedanımlanmıştır.Orantılılık ilkesi, araç ile amacın arasında ölçülü bir orantının bulunması durumudur⁹. Kullanılan aracın ulaşılmak istenen amaç bakımından orantısız olmaması gerekmektedir. Biyometrik veri işleme noktasında, müdahalenin ağırlığı ile müdahaleyi haklı kılacak sebepler arasında ölçülülüğün bulunması gerekmektedir; yani kullanılan araç neticesinde ilgili kişilere orantısız müdahalelerde bulunulmamalıdır¹⁰. Birden fazla aracın bulunduğu durumda en uygun olan aracın seçilmesi, orantılılığı ifade etmektedir.

Tehlikeli virüsler hakkında araştırma yapan bir şirkette, laboratuvarın ancak başarılı bir parmak izi ve iris taraması doğrulamasından sonra açılan kapılarla güvence altına alındığını düşünelim. Bu yöntemin yalnızca belirli risklere aşına olan prosedürler konusunda eğitilen ve şirket tarafından güvenilir bulunan kişilerin bu tehlikeli malzemeleri deneyebilmesini sağlamak için uygulanması durumunda şirketin, o yasaklı alana erişimle gelen güvenlik risklerinin azaltılabileceğini garanti etmek için yalnızca yetkili kişilerin girebileceğinden emin olma konusundaki meşru menfaati ilgili kişilerin biyometrik verilerinin işlenmemesi isteğini önemli ölçüde geçersiz kılacaktır.

- d) Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin gecikmeksizin/derhal imha edilmesi.
- e) İşleme amacı doğrultusunda sınırlı olmak üzere; veri sorumlularının Kanunun 10 uncu maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi: Bilindiği üzere, aydınlatma yükümlülüğünün yerine getirilmesine ilişkin olarak Kanunun 10 uncu maddesinin yanı sıra “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*” 10.03.2018 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

9 Metin, Y. s.13

10 Metin, Y. s.14

Anılan mevzuat hükümlerine riayet edilmekle birlikte, biyometrik verilerin önemine binaen biyometrik veri işleyecek veri sorumlularının ayrıca hangi biyometrik verileri hangi hukuki sebeple ve hangi amaçla alındığı, bu verilerin önemi, ihlâl durumunda ortaya çıkabilecek sonuçların neler olabileceği (biyometrik verilerin işlenmesine yönelik riskler) hususlarına ilişkin olarak ilgili kişileri ayrıca aydınlatmalıdır.

- f) Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının Kanuna uygun şekilde alınmış olması: Kanunun “Tanımlar” başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde açık rıza, “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” şeklinde tanımlanmıştır. Veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi gerekmektedir. Bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerekir. Kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekir¹¹. Bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka verinin işlenmesinden önce yapılması gerekir.

Diğer yandan, açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı olması gerekmektedir. Açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir ürün ve/veya hizmetin sunumu (ya da herhangi bir üründen ve/veya hizmetten yararlandırılması) ilgili kişi tarafından açık rıza verilmesi şartına bağlanmamalı, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilir verilmediğinin dikkatle değerlendirilmesi gerekmektedir¹². Örneğin, işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez¹³.

11 Kişisel Verileri Koruma Kurumu. “Açık Rıza”, s. 5

12 Kişisel Verileri Koruma Kurumu. “Açık Rıza”, s. 6

13 Kişisel Verileri Koruma Kurumu. “Açık Rıza”, s. 6

2. Yukarıda sayılan bütün ilkelerin sağlandığı hususu veri sorumlusu tarafından kayıt altına alınıp belgelendirilmelidir.
3. Gerekmediği takdirde, biyometrik veri alınırken genetik veri (kan, tükürük vb.) alınmamalıdır.
4. Biyometri türünün veya türlerinin seçiminde (iris, parmak izi, elin damar ağı, vb.) tercih edilen biyometrik veri türünün veya türlerinin diğerleri yerine neden seçildiğine dair gerekçeler ve belgeler sunulmalıdır.
5. Kanununun 4 üncü maddesinin birinci fıkrasının (d) bendinde yer alan ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereği, kişisel verilerin işlenmesinde azami süre belirlenmelidir. Bu çerçevede, sürelerin belirlenmesinde mevzuattan kaynaklanan süreler olabileceği gibi, mevzuat kaynaklı olmayan ancak veri sorumlularının tayin edeceği süreler de olabilir. Bununla birlikte, biyometrik özelliğin bütün çeşitleri (ham ve türetilmiş vb. kayıtlar) gereken süre boyunca işlenmeli; söz konusu verilerin ne kadar süre boyunca tutulacağı nedenleri ile birlikte kişisel veri saklama ve imha politikasında veri sorumlusu tarafından açıklanmalıdır.

BİYOMETRİK VERİ GÜVENLİĞİ

Biyometrik veri işleyen veri sorumlularının; kanun, yönetmelik, tebliğ ve kurul kararlarında yer alan kişisel veri güvenliği ile ilgili hususlara dikkat etmeleri zorunludur. Bu çerçevede, özel nitelikli kişisel veri niteliğini haiz verilerin işlenmesinde; Kurulun “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*”e ilişkin 31/01/2018 tarihli ve 2018/10 sayılı kararında belirtilen tedbirlerin alınması zorunludur. Bununla birlikte, veri sorumlularına yol göstermek amacıyla Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan rehber dokümanlarda tavsiye edilen tedbirlerden uygun olanların da dikkate alınması gerekir. Bu kapsamda veri sorumlusu, verilerin niteliği ve veri işleminin ilgili kişi açısından oluşturacağı muhtemel risklerle ilgili olarak, verilerin güvenliğini sağlamak amacıyla gerekli teknik ve idari tedbirleri almalıdır. Veri sorumlularının, bahse konu mevzuat ve rehberlerdeki veri güvenliği tedbirlerine ilaveten biyometrik veri işleme hususunda aşağıdaki tedbirleri de alması gerekmektedir.

1. Teknik Tedbirler:

- a) Biyometrik veriler bulut sistemlerinde ancak kriptografik yöntemler kullanılarak muhafaza edilmelidir.
- b) Türetilmiş biyometrik veriler, orijinal biyometrik özelliğın yeniden elde edilmesine izin vermeyecek biçimde saklanmalıdır.
- c) Biyometrik veriler ve şablonları güncel teknolojiye uygun olarak, yeterli güvenliğı sağlayacak kriptografik yöntemlerle şifrelenmelidir. Şifreleme ve anahtar yönetimi politikası açıkça tanımlanmalıdır.
- ç) Veri sorumlusu sistemi kurmadan önce ve herhangi bir değışiklikten sonra, oluşturulacak test ortamlarında sentetik veriler (gerçek olmayan) aracılığıyla sistemi test etmelidir.
- d) Veri sorumlusu, test amaçlı olarak yapacağı çalışmalarda biyometrik verilerin kullanımını gerekli olanla sınırlamalıdır. Tüm veriler en geç testlerin sonunda silinmelidir.
- e) Veri sorumlusu, sisteme yetkisiz erişilmesi durumunda sistem yöneticisini ikaz eden ve/veya biyometrik verileri silen ve rapor veren önlemler uygulamalıdır.
- f) Veri sorumlusu sistemde sertifikalı teçhizat, lisanslı ve güncel yazılımlar kullanmalı, öncelikli olarak açık kaynak kodlu yazılımları tercih etmeli ve sistemdeki gerekli güncellemeleri zamanında yapmalıdır.
- g) Biyometrik veriyi işleyen cihazların kullanım ömrü izlenebilir olmalıdır.

- ğ) Veri sorumlusu biyometrik veriyi işleyen yazılım üzerindeki kullanıcı işlemlerini izleyebilmeli ve sınırlayabilmelidir.
- h) Biyometrik veri sisteminin donanımsal ve yazılımsal testleri periyodik olarak yapılmalıdır.

2. İdari Tedbirler:

- a) Biyometrik çözümü kullanamayan (biyometrik verilerin kaydedilmesi veya okunması imkansız, kullanımı zorlaştıran handikap durumu, vb.) veya kullanmaya açık rızası olmayan ilgili kişiler için herhangi bir kısıtlama veya ek maliyet olmaksızın alternatif bir sistem sağlanmalıdır.
- b) Biyometrik yöntemlerle kimlik doğrulamanın yapılamaması ya da başarısızlığı durumunda gerçekleştirilecek bir eylem planı oluşturulmalıdır (bir kimliği doğrulayamama, güvenli bir alana girme yetkisi eksikliği, vb.).
- c) Yetkili kişilerin biyometrik veri sistemlerine erişim mekanizması kurulmalı, yönetilmeli ve sorumluları belirlenerek belgelendirilmelidir.
- ç) Biyometrik veri işleme sürecinde yer alan personel biyometrik verilerin işlenmesi hususunda özel eğitimler almalı ve söz konusu eğitimler belgelendirilmelidir.
- d) Çalışanların sistem ve servislerdeki muhtemel güvenlik zafiyetleri ve söz konusu zafiyetler sonucu oluşabilecek tehditleri bildirebilmesi için resmi bir raporlama prosedürü oluşturulmalıdır.
- e) Veri sorumlusu bir veri ihlali durumunda uygulanmak üzere acil durum prosedürü oluşturmalı ve ilgili herkese duyurmalıdır.

KAYNAKLAR

- Satapathy S. C. & Joshi A. (2017). Information and Communication Technology for Intelligent Systems (ICTIS 2017), Bhatnagar S. Cooperative Multimodal
- Approach for Identification – (Volume 1)
Metin, Yüksel, (2017) Temel Hakların Sınırlandırılması ve Ölçülülük. SDÜHFD, Cilt:7, Sayı: 1
- Kişisel Verileri Koruma Kurumu, “Açık Rıza”