KVKK Yayınları No: 50

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BANKACILIK SEKTÖRÜ İYİ UYGULAMALAR REHBERİ

ARALIK 2024

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BANKACILIK SEKTÖRÜ İYİ UYGULAMALAR REHBERİ

ARALIK 2024

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BANKACILIK SEKTÖRÜ İYİ UYGULAMALAR REHBERİ

KVKK Yayınları No: 50

Kişisel Verileri Koruma Kurumu
Adres: Nasuh Akar Mahallesi 1407. Sokak No: 4 Balgat / ANKARA / TÜRKİYE
Telefon: +90 312 216 50 00
Web: www.kvkk.gov.tr

Baskı: G.M. Matbaacılık ve Tic. A.Ş.
100. Yıl Mah. MAS-SİT 1.Cad. No: 88 Bağcılar - İstanbul
Tel.: 0212 629 00 24 Sertifika No: 45463
Baskı Tarihi: Ocak 2025

Bu rehber, Kişisel Verileri Koruma Kurumu ve Türkiye Bankalar Birliği tarafından işbirliği içerisinde hazırlanmıştır.


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

İÇİNDEKİLER

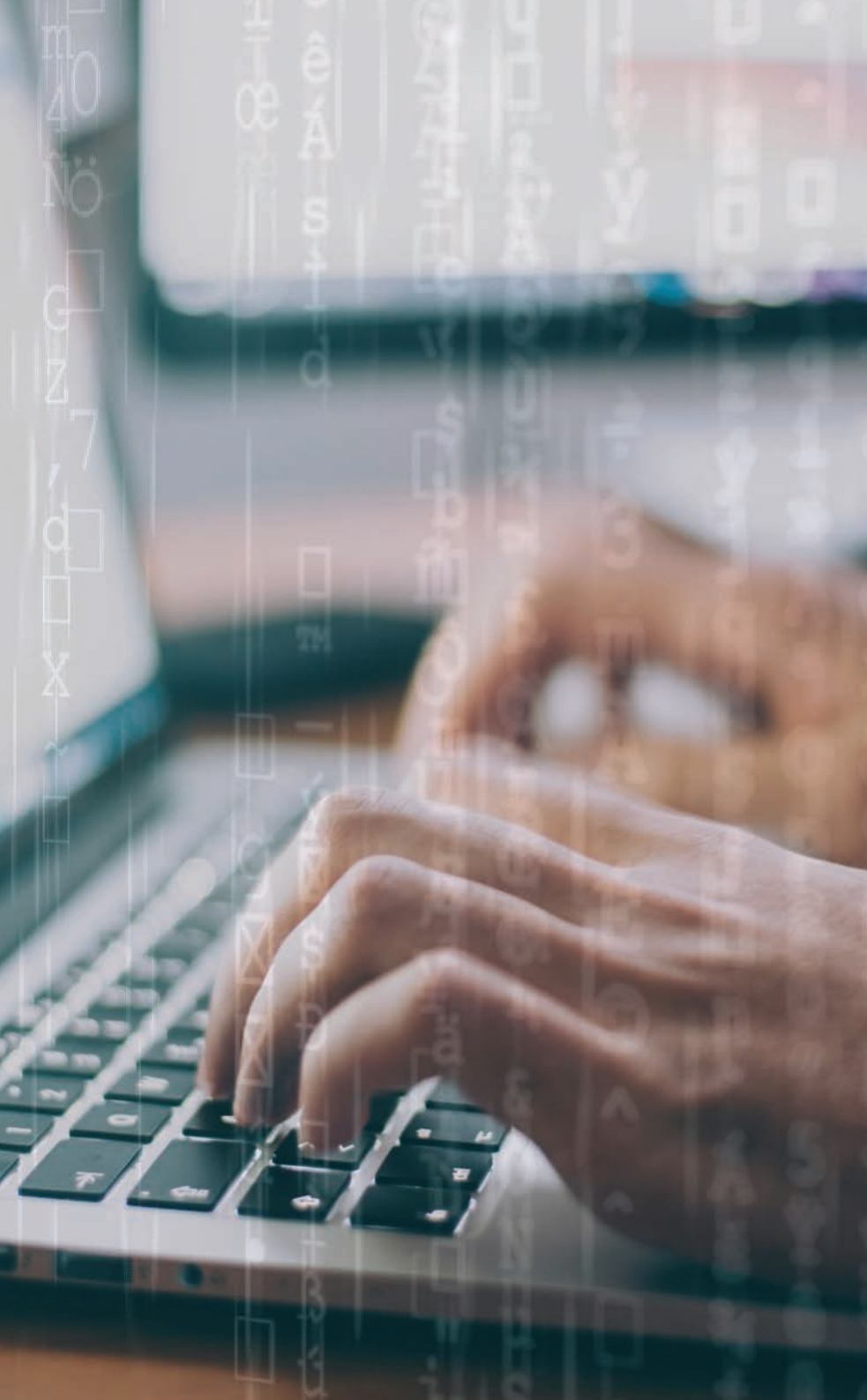
6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN BANKACILIK SEKTÖRÜNDE UYGULANMASI 13
I. Giriş 13
II. Kurum Tanıtımı 14
III. Amaç ve Kapsam 16
IV. Veri Sorumlusu-Veri İşleyen İlişkileri 17
1. Veri Sorumlusu- Veri İşleyen Arasında Yapılacak Olan Veri İşleme Sözleşmesi 21
2. Destek Hizmetleri 24
3. İştirakler ve Bağlı Ortaklıklar 25
4. Açık Bankacılık 25
5. Bankaların Acente Sıfatıyla Hareket Ettiği Durumlar 26
V. İlgili Kişi 28
VI. İşlenen Kişisel Veriler 29
VII. Kişisel Veri İşleme Şartları 30
1. Açık Rıza 31
1.1. Açık Rızanın Unsurları 33
1.1.1. Belirli Bir Konuya İlişkin Olma 33
1.1.2. Özgür İradeyle Açıklanmış Olma 33
1.1.3. Bilgilendirmeye Dayanma 34
1.2. Kanala Özgü İyi Uygulama Örnekleri 34
1.2.1. Şube 35
1.2.2. ATM 35
1.2.3. İnternet/Mobil Bankacılık 35
1.2.4. Çağrı Merkezi 35
1.2.5. SMS 35
1.2.6. Elektronik Posta 36
2. Kanunlarda Öngörülmesi ve Hukuki Yükümlülüğün Yerine Getirilmesi 36
2.1. Bankaların Tabi Olduğu Mevzuata İlişkin Yükümlülüklerinin Değerlendirilmesi 38
2.1.1. Mevzuat 38
2.1.2. Bankacılık Faaliyetleri Kapsamında Kanunlarda Öngörülen İşlemeler 38

2.1.2.1. Bankacılık Kanunu Madde 73 ve Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik 39
2.1.2.2. Risk Değerlendirmesi 42
2.1.2.3. Diğer Kanuni Yükümlülükler Gereği Veri İşleme ve Paylaşım 43
2.1.3. İyi Uygulamalar 45
3- Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesi 45
4- Meşru Menfaat 46
4.1. Bilgi Güvenliğinin Sağlanması Amacıyla 49
4.1.1. Dolandırıcılık Tedbirleri 50
4.2. Bankacılık Alanında Müşteri Gruplarının (Segmentasyon) Belirlenmesi Amacıyla 50
4.3. Müşterilere Hitap Eden Ürün Hizmetlerin Tespiti Amacıyla 51
4.4. Strateji Çalışmalarının Yürütülmesi 53
4.5. Müşteri Memnuniyetinin Sağlanması 56
5- Bir Hakkın Tesisi ve Korunması İçin Zorunlu Olma 56
6- Bankalarca İşlenen Özel Nitelikli Kişisel Veriler 57
6.1. Özel Nitelikli Kişisel Veriler – Genel Olarak 57
6.1.1. Mevzuat 57
6.1.2. Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Yeterli Önlemler 60
6.2. Bankacılık Sektöründe Özel Nitelikli Kişisel Verilerin İşlenmesi 63
6.2.1. Kimlik Belgesi Suretleri 63
6.2.2. Sağlık Raporları 65
6.2.3. Adli Sicil Kayıtları ve Ceza Mahkumiyeti ve Güvenlik Tedbirleriyle İlgili Mahkeme Kararları 66
6.2.4. Çalışanları Sağlık Verileri 68
6.2.5. Sigorta Acentesi Sıfatıyla Alınan Sağlık 68
6.3. Kimlik Doğrulamada Kullanılan 69
VIII. Kişisel Verilerin Aktarılması 72
1. Kişisel Verilerin Yurt İçinde Aktarılması 72
1.1. KVKK Madde 8/3 Uyarınca Yapılabilecek Kişisel Veri Aktarımları 76
1.1.1 Bankalardan Bilgi Talep Etmeye Yetkili Mercilere Gerçekleştirilen Kişisel Veri Aktarımları 77
1.1.2. Şüpheli İşlem Bildirim Zorunluluğu Çerçevesinde Gerçekleştirilen Kişisel Veri Aktarımları 80

1.1.3. Ana Ortak/Bağlı Ortaklıklara Gerçekleştirilen Kişisel Veri Aktarımları 81
1.1.4. Muhtemel Alıcılara Gerçekleştirilen Kişisel Veri Aktarımları 81
1.1.5. Bankalar ve Finansal Kuruluşlara Gerçekleştirilen Kişisel Veri Aktarımları 82
1.1.6. Risk Merkezi, Bankalar Arası Kart Merkezi ve Kredi Kayıt Bürosu'na Gerçekleştirilen Kişisel Veri Aktarımları 82
1.1.7. İştiraklere Gerçekleştirilen Kişisel Veri Aktarımları 82
1.1.8. Değerleme, Derecelendirme ve Destek Hizmeti Kuruluşlarına Gerçekleştirilen Kişisel Veri Aktarımları 83
1.2. İş Ortaklarına Gerçekleştirilen Kişisel Veri Aktarımları 83
2- Yurtdışına Veri Aktarımı 84
2.1. Yurtdışına Veri Aktarımı Yöntemleri 84
2.1.1. Yeterlilik Kararı 85
2.1.2. Uygun Güvenceler 85
2.1.3. Arızi Haller 87
2.1.4. Kanunun 9 uncu Maddesinin Onuncu Fıkrası Uyarınca Yapılacak Aktarımlar 89
IX. Genel İlkeler 91
X. Veri Sorumlusunun Yükümlülükleri 94
A. Aydınlatma Yükümlülüğü 94
1- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde İçerik 94
1.1. Katmanlı Aydınlatma 97
2- Aydınlatma Yükümlülüğünün Yerine Getirilme Zamanı 99
3- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Usul 99
3.1. Şube 100
3.2. İnternet Sitesi 100
3.3. İnternet Şube 101
3.4. Mobil Şube ve Mobil Uygulama 101
3.5. Çağrı Merkezi/IVR 101
3.6. Elektronik Posta 102
3.7. Fiziki Posta 102
3.8. SMS 102
3.9. ATM 102
4- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Özel Durumlar 103

4.1. İmza Yetkilileri ve Gerçek Faydalanıcıların Aydınlatılması 103
4.2. Risk Grubu'ndakilerin Aydınlatılması 103
4.3. Varlığın Sahibi Dışındaki Kişilere İlişkin Kişisel Verilerin ve Çek-Senetlerde Son Ciranta Dışındaki Kişilerin Kişisel Verilerinin İşlenmesi 104
4.4. Maaş Ödeme Anlaşmaları 105
4.5. Kredi Kartları ve Banka Kartları İşlemleri 106
B. Veri Sorumluları Sicili, Sicile Kayıt ve Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü 106
1- Bankacılığa Özgü Veri Kategorileri 108
2- Kişi Grupları 109
3- Alıcı Grupları 109
4- Azami Süreler 109
C. Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi 111
1- Bankacılıkta Bilgilerin Saklanması 111
2- İşleme Amacının Ortadan Kalkması 112
3- İmha Yöntemleri 115
D. Veri Güvenliği 119
1- Bankaların Yasal Mevzuattan Kaynaklanan Yükümlülükleri 119
1.1. Bankacılık Kanunu 119
1.2. Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik 119
1.3. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik 119
1.4. Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik 119
1.5. Bilgi Güvenliğine İlişkin Teknik ve İdari Önlemler 119
2- Denetim 126
E. İlgili Kişinin Hakları ve Şikâyetlerin Yönetilmesi 128
1- Veri Sorumlusu Temsilcisi 128
2- Başvuru ve Şikayetlerin Alınması ve Yanıtlanması 129
2.1. Veri Sorumlusuna Başvuru 129
2.1.1. Şekil ve Usul 130
2.2. Kurula Şikayet 132
2.2.1. Kimlik Tespiti/Doğrulama 133


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU




KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN BANKACILIK SEKTÖRÜNDE UYGULANMASI

I. Giriş

Bankalar, bireylerin gündelik hayatında sıklıkla muhatap oldukları kuruluşların başında gelmekte olup bankacılık faaliyetleri kapsamında bankalar tarafından çeşitli kanallar üzerinden yoğun bir biçimde kişisel veri elde edilmekte ve bunu müteakiben söz konusu kişisel veriler çeşitli amaçlarla işlenmektedir. Bu sebeple, hâlihazırda bankacılık mevzuatına uygun olarak faaliyetlerini yürüten bankaların 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun/Kanun) ve ilgili ikincil mevzuat çerçevesinde uyması gereken usul ve esaslar ile yerine getirmesi gereken yükümlülüklerin iyi uygulama örnekleri vasıtasıyla ortaya konulması hususunda bir ihtiyaç bulunmaktadır.

Diğer taraftan, her geçen gün kişisel verilerden yararlanmak suretiyle daha verimli iş modelleri oluşturulmakta ve bireylere sunulan ürün ve hizmetler iyileştirilmektedir. Benzer şekilde, bankalar da daha etkin iş süreçleri oluşturmak ve müşteri memnuniyetini en üst düzeye çıkarmak adına teknolojik gelişmeler sonucu ortaya çıkan karmaşık ve ileri düzey kişisel veri işleme tekniklerini kullanmaktadır. Özellikle dijital bankacılık uygulamalarının yaygınlaşmasıyla bankalar tarafından gerçekleştirilen işleme faaliyetlerine konu kişisel veri kategorileri çeşitlenmiş ve özel nitelikli kişisel veriler başta olmak üzere hukuka aykırı olarak elde edilmesi halinde ilgili kişiler nezdinde telafisi güç zararların doğmasına neden olabilecek kişisel veriler de bankacılık faaliyetleri kapsamında işlenmeye başlamıştır. Bununla birlikte, bankaların kişisel veri toplama vasıtaları da eş zamanlı olarak çoğalmış olup kişisel verilerin elde edilmesi kolaylaşmıştır.

Bu çerçevede, bankalar tarafından yoğun bir şekilde kişisel veri işleme faaliyeti gerçekleştirildiği ve bu kapsamda anayasal güvence altında bulunan kişisel verilerin korunmasını isteme hakkı bağlamında ilgili kişilerin maruz kaldığı risk derecesi göz önünde bulundurularak; Kişisel Verileri Koruma Kurumu ve Türkiye Bankalar Birliği bünyesinde çalışma grupları kurulmuştur. Söz konusu çalışma grupları arasında periyodik toplantılar

gerçekleştirilmiş ve Bankacılık Sektöründe Kişisel Verilerin Korunmasına ilişkin iyi Uygulamalar Rehberi sektörle işbirliği içinde hazırlanmıştır.

II. Kurum Tanıtımı

Kanun'da belirtilen görevleri yerine getirmek üzere kurulan, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu (Kurum);

- Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirmek ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak,
- İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak,
- Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak, yıllık faaliyet raporunu Cumhurbaşkanlığına ve Türkiye Büyük Millet Meclisi insan Haklarını inceleme Komisyonuna sunmak,
- Kanunlarla verilen diğer görevleri yerine getirmek,

hususlarında görevli ve yetkili kılınmıştır. Kişisel Verileri Koruma Kurulu (Kurul) ve Başkanlık şeklinde teşkilatlanan Kurumun karar organı Kuruldur. Kurul, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirmekte ve kullanmakta olup görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. Dokuz üyeden oluşan Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilmekte ve 6698 sayılı Kanun'un 22. maddesinde sıralanan görev ve yetkiler, Kurul tarafından yerine getirilmektedir. Bu görev ve yetkiler mezkûr düzenlemede;

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,
- Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak,

- Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak,
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek,
- Veri Sorumluları Sicilinin tutulmasını sağlamak,
- Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak,
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak,
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak,
- Kanunda öngörülen idari yaptırımlara karar vermek,
- Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek,
- Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek,
- Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak,
- Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak,
- Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak,
- Kanunlarla verilen diğer görevleri yerine getirmek,

şeklinde ifade edilmiştir.

Yine 26/4/2018 tarihinde yayımlanan Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği'nin Kurulun görev ve yetkileri'nin düzenlendiği 7 nci maddesinde kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek, kişisel verilerin korunması konusunda kurum ve kuruluşları bilgilendirmek ve kamuoyuna yönelik farkındalık faaliyetleri gerçekleştirmek, üniversiteler ve ilgili diğer yurtiçi ve yurtdışı kurum ve kuruluşlarla işbirliği ve koordinasyon çalışmaları yürütmek görevlerine yer verilmiştir.

III. Amaç ve Kapsam

Bu Rehberin amacı bankalar tarafından yürütülen kişisel veri işleme faaliyetlerinin 6698 sayılı Kanuna ve bu Kanuna dayanılarak Kurul tarafından çıkartılan ikincil mevzuata uygun olarak gerçekleştirilmesi konusunda veri sorumlusu bankaları yönlendirmek ve bu çerçevede iyi uygulama örnekleri oluşturmaktır. Bu Rehber, bankaların kişisel verilerin korunması alanında uyması gereken usul ve esaslar ile yerine getirmesi gereken yükümlülüklere ilişkin genel açıklamaları içermekte olup bankaların 6698 sayılı Kanuna ve ilgili ikincil mevzuata uyum yükümlülüğü devam etmektedir. Bununla birlikte Kurul, kendisine intikal ettirilen şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen yapacağı incelemede somut olayın özelliklerini göz önünde bulundurarak değerlendirmesini yapacaktır.

IV. Veri Sorumlusu-Veri İşleyen İlişkileri

Veri sorumlusu; Kanunun 3. maddesinin birinci fıkrasının (ı) bendinde kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. Veri sorumlusu veri işleme faaliyetinin temel araçlarını, veri işlemenin neden ve nasıl olacağını belirler, veri işleme süreçlerinin her anında serbestçe karar verme yetkisine sahiptir.

Gerçek kişilerin[1] yanı sıra kamu kurumu, şirket, dernek veya vakıf gibi tüzel kişilerin veri sorumlusu olması mümkündür. Tüzel kişiliğe sahip olmayan adi ortaklık veya apartman yönetimi gibi oluşumlarda veri sorumlusunun, bu oluşumu oluşturan gerçek ya da tüzel kişiler olduğu kabul edilmektedir.

Veri işleyen; Kanunun 3. maddesinin birinci fıkrasının (ğ) bendinde veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir. Veri işleyen kişisel veri işleme faaliyetini, veri sorumlusunun belirlemiş olduğu temel amaç ve vasıtalar ile ve/veya talimatlara uyarak gerçekleştirir.

Buna göre veri sorumlusu, kişisel verilerin işlenmesine ilişkin her türlü kararı verme yetki ve sorumluluğuna sahipken veri işleyen ise onun verdiği talimatlar doğrultusunda hareket eden, ondan bağımsız bir gerçek veya tüzel kişidir.

Veri işleyen olma bakımından en önemli kriterlerden biri, bir veri sorumlusu adına hareket etmektir. Veri işleyen, verinin işlenmesinde doğrudan menfaat sahibi olmamalı, yalnızca veri sorumlusunun adına hareket ediyor olmalıdır. Tabii bu noktada, dolaylı ekonomik menfaatinin bulunması, yani vermiş olduğu hizmet karşılığında veri sorumlusundan ücret/

[1]"Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 14/01/2020 tarihli ve 2020/26 sayılı Karar Özeti. www.kvkk.gov.tr.
Bir doktor tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 07/11/2019 tarihli ve 2019/332 sayılı Karar Özeti. www.kvkk.gov.tr .

komisyon vb. almış olması, bir kıstas olarak kabul edilmemelidir.

Veri sorumlusu/veri işleyen sıfatının tespiti için aşağıdaki hususlara kimin karar verdiği dikkate alınmalıdır[2]:

- Kişisel verilerin toplanması ve toplama yöntemi,
- Toplanacak kişisel veri türleri,
- Hangi bireylerin kişisel verilerinin toplanacağı,
- Kişisel verinin işlenmesine ve kimin işleyeceğine karar verme,
- İşleme faaliyetinin temel unsurlarına karar verme (hangi kişisel verilerin toplanacağı, toplanan verilerin hangi amaçlarla kullanılacağı ve ne şekilde işleneceği, verilerin ne kadar süreyle saklanacağı, veri saklama politikasının ne şekilde olacağı, verilere kimlerin erişme yetkisi olacağı, alıcıların kim olacağı gibi hususlar işlemenin temel unsurlarına örnek olarak gösterilebilir)
- Toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı,
- Kişisel verilerin işlenmesinde üst düzeyde, herhangi bir emir ve talimat almadan karar verebilme,
- İlgili kişilerle doğrudan muhatap olma,
- Kendi adına veri işleme faaliyetini yürütecek bir veri işleyen atama,
- İşleme faaliyetinden menfaat sağlama.

Veri işleme faaliyeti gerçekleştirilen her bir süreç özelinde yukarıda verilen hususlardan çoğunu gerçekleştiren taraf veri sorumlusu olarak nitelendirilecektir.

Veri işleyenin tespiti için aşağıdaki hususlar değerlendirilmelidir:

- Kişisel veri işlemek için başkasından talimat alınması,
- Kişisel verilerin kişilerden toplanması sürecinde karar verme yetkisine sahip olmamak,
- Kişisel verilerin kullanım amaçlarının belirlenmemesi,
- Verilerin ne şekilde ifşa olabileceğine, kimlerin bu verilere

[2] "Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceğine" ilişkin Kişisel Verileri Koruma Kurulu'nun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti. www.kvkk.gov.tr.

erişebileceğine karar verme yetkisine sahip olmamak,
- Veri saklama sürecine karar verme yetkisine sahip olmamak,
- Veri işlemenin sonuçlarından sorumlu olmaması,
- Veri sorumlusu ile yapılacak sözleşme gibi yasal bağlayıcılığı olan anlaşmalar çerçevesinde veri sorumlusunun verdiği yetkiler çerçevesinde kişisel verilerin işlenmesine yönelik birtakım karar verme mekanizmalarının söz konusu olması.

Bankalar gerçekleştirdikleri kişisel veri işleme faaliyetleri kapsamında veri sorumlusu veya veri işleyen sıfatını haiz olabilir. Bankalar, 5411 sayılı Bankacılık Kanunu'nun 4. maddesi uyarınca gerçekleştirdiği bankacılık faaliyetleri açısından veri sorumlusudur. Bununla birlikte, acente ve aracı kuruluş olduğu sigorta, bireysel emeklilik, yatırım ürünleri, uluslararası hızlı para transferi ile fatura/vergi/harç ödeme faaliyetlerinde bulunduğu durumlarda bankanın veri sorumlusu ya da veri işleyen olduğuna karar verilirken somut olayın koşulları değerlendirilerek yorum yapılması gerekir.

Bankaların "veri sorumlusu" sıfatını haiz olduğu veri işleme faaliyetlerine Veri Sorumluları Sicili'nde yer verilir. Bankaların "veri sorumlusu" olmamaları nedeniyle Veri Sorumluları Sicili'nde yer verilmeyen ancak "veri işleyen" sıfatını haiz olduğu veri işleme faaliyetlerine ise Veri Sorumluları Sicili'nde yer verilmesine gerek bulunmamaktadır. Bankaların "veri işleyen" sıfatını haiz olduğu veri işleme faaliyetlerinde uygun güvenlik düzeyini temin etme sorumluluğuna ek olarak üstlendiği sorumluluklar ise veri sorumlusu ile veri işleyen arasında akdedilen sözleşmeler ile belirlenmektedir. Dolayısı ile bankaların her somut olay bazında taraflar arasındaki ilişki ve veri akışını değerlendirmek suretiyle veri işleyen olup olmadığına karar verilmelidir.

Kurulun 13/04/2021 tarih ve 2021/359 sayılı Kararı ve diğer emsal kararlarında da görüleceği üzere, veri sorumlusu ile veri işleyen ayrımında yukarıda yer verilen hususlar göz önüne alınarak belirleme yapılmaktadır[3].

[3] "Yönetim Hizmeti Sunan Şirketin Site Temsilciler Kurulu ile akdettiği sözleşme kapsamında ilgili kişinin ikamet ettiği sitede yönetim hizmetleri verdiği, bu anlamda söz konusu hizmetlerin ifası gereği Yönetim Hizmeti Sunan Şirketin 3. kişilerle sözleşme yapabileceği, bu sözleşmeler

Örneğin; personelin maaşını ödemek için kimlik, iletişim ve banka hesap bilgilerini işleyen bir şirket (ya da özel kişi), hangi kişinin hangi verilerini işleyeceğine karar vermekte; bu verileri nasıl işleyeceğini de (bir veri tabanında ya da bir alanda da tutmak gibi) kendisi belirlemektedir. Kişisel verilerin neden (amaç) ve nasıl (yöntem) işlendiğine karar veren şirket (ya da gerçek kişi) veri sorumlusudur[4].

Her ne kadar Kanunda ve ilgili mevzuatta tanımlanmamış olsa da Kurul kararlarında[5] tek bir veri kayıt sistemi çerçevesindeki veri işleme faaliyetlerinde, bu faaliyetlerin amaç ve vasıtalarının birden fazla kişi tarafından müştereken belirlenmesi durumunda aynı veri işleme faaliyeti bakımından birden fazla veri sorumlusu olabileceği kabul edilmiştir.

Ancak, her ortak veri işleme faaliyeti doğrudan müşterek bir sorumluluk anlamına gelmez veya verileri birbirine aktaran kişiler ortak veri sorumlusu sayılmaz. Ortak veri sorumlusu olabilmek için veri işleme faaliyetinin amacını ve vasıtaları yani faaliyette kullanılacak aracı ortak belirlemek gerekir. Zaten, ortak veri sorumluluğunun belirlenmesinde esas alınacak yegâne ölçüt de budur.

Müşterek veri sorumluları arasında yükümlülüklerin belirlenmesinde taraflar arasında sözleşme yapılması önemlidir. Bu kapsamda ortak veri sorumluları arasında akdedilecek sözleşmelerde, Kanunda veri sorumlusuna yüklenen yükümlülüklerin kim tarafından ne şekilde yerine getirilmesi

---

kapsamında sorumluluğun Yönetim Hizmeti Sunan Şirkete ait olduğu, Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen uygulama/ikinci uygulama ile hizmet sözleşmesi akdettiği ve bu sözleşmenin eki niteliğinde olan KVKK Protokolünde hizmet sözleşmesinde Yönetim Hizmeti Sunan Şirketin veri sorumlusu sıfatını haiz olduğuna yer verildiği dikkate alındığında Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen ikinci uygulama ile yaptığı sözleşme kapsamında kişisel verilerin işlenme amaç ve yöntemini belirleyen kişi olarak veri sorumlusu sıfatını taşıdığı, Uygulama Hizmetini Sunan Şirketin ise Yönetim Hizmeti Sunan Şirketin verdiği yetki kapsamında onun adına veri işleme faaliyetini gerçekleştiren veri işleyen sıfatını haiz olduğu, www.kvkk.gov.tr

[4] Örneklerle Kişisel verilerin Korunması, Kişisel Verileri Koruma Kurumu, KVKK Yayınları No:29, s.59 www.kvkk.gov.tr

[5] Kişisel Verileri Koruma Kurulu'nun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti. www.kvkk.gov.tr

gerektiğinin şeffaf bir şekilde düzenlenmesi halinde, bu düzenlemeler tarafların sorumluluk sınırlarının belirlenmesi açısından dikkate alınır. Ancak ilgili kişi, veri koruma hukukundan doğan haklarını veri sorumlularının her birine karşı ileri sürebilir.

1. Veri Sorumlusu- Veri İşleyen Arasında Yapılacak Olan Veri İşleme Sözleşmesi

Veri işleme hükümlerine veri sorumlusu ile veri işleyen arasındaki hizmet sözleşmesi içeriğinde yer verilebileceği gibi hizmet sözleşmesine ek mahiyette ayrı bir düzenleme yapılması da mümkündür.

Veri sorumlusu veri işleyen arasındaki sözleşmelerde asgari olarak aşağıdaki hususlara yer verilmesi ve sözleşmenin yazılı olması önerilmektedir:

- İşleme faaliyetinin konusu,
- Kişisel veri işleme amacı,
- Kişisel verilerin işlenme süresi,
- Kişisel verilerin türü,
- Veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hüküm içermesi, (Kişisel Veri Saklama ve İmha Politikasına uygun olması)
- Tarafların süresiz sır saklama yükümlülüğüne tabi olacağı,
- Veri işleyenin ilgili kişilere haklarının kullandırılmasına ilişkin olarak veri sorumlusuna yardım etme yükümlülüğü,
- Gerekli özeni gösterme borcu,
- Sözleşmenin ve/veya kişisel verinin elde edilme amacının sona ermesini müteakip veri işleyenin verileri silme veya iade etme yükümlülüğü/süresiz sorumluluk,
- Bankaların, "veri sorumlusu" olduğu durumlarda, veri işleyenlere gerekli denetimleri yapma hakkını haiz olduğu,
- Herhangi bir veri ihlali olması durumunda veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olduğu.

Bankaların "veri işleyen" olduğu durumlarda, banka ve müşteri sırrına

ilişkin ilgili kanun ve benzeri kanuni yükümlülükler nedeniyle denetime izin verilmeyebileceğinin yapılacak sözleşmede kabulüne (bankalardaki denetim gerekliliklerinin bağımsız denetim şirketlerinden veya bankanın iç denetim birimlerinden, faaliyetlerin uyumlu olduğuna ilişkin alınacak raporlarla sağlanabilmesi imkânı saklı kalmak kaydıyla) dikkat edilmelidir.

Ayrıca Kurumun "Veri Sorumlusu ve Veri işleyen Rehberi"nde[6] örnek olarak belirtildiği üzere, veri sorumlusu veri işleyen arasındaki sözleşmelerde, veri sorumlusu tarafından aşağıda sayılan bazı hususlarda karar verme yetkisi veri işleyene bırakılabilir:

- Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri.

Veri sorumlusu ve veri işleyen ilişkisinde aydınlatma yükümlülüğünün kim tarafından gerçekleştirileceği hususu da veri sorumlusunun takdirine bırakılmıştır. Kanunun 10 uncu maddesi uyarınca veri sorumlusu, kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aydınlatma yükümlülüğünü yerine getirebilir. Buna göre veri sorumlusu, aydınlatma yükümlülüğünü bizzat kendisi yerine getirilebileceği gibi veri işleyen aracılığıyla da gerçekleştirebilir.

İlaveten, aşağıda örnek olarak belirtilen, veri sorumlusunun kanundan kaynaklanan yükümlülüklerinin yerine getirilmesinde veri işleyenden destek alınacağına veya diğer veri işleme esaslarına dair veri işleme sözleşmesine hükümler konulabilir:

- Veri işleyenin veri güvenliğini sağlama konusunda alacağı tedbirlerin tespiti,

[6] Veri Sorumlusu ve Veri İşleyen Rehberi s. 3.

- Şahsen ifa yükümlülüğü/alt veri işleme yetkisinin bulunup bulunmadığı, alt veri işleme yetkisi mevcut ise veri işleyen ile alt veri işleyenlerle akdedilecek sözleşmelerde hangi hususlara yer verilmesi gerektiği,
- İlgili kişileri aydınlatma yükümlülüğünün veri işleyen aracılığı ile yerine getirilmesi halinde veri işleyenin yükümlülükleri (örnek olarak, acentelik ilişkileri kapsamında veri sorumlusu sigorta şirketi tarafından hazırlanan aydınlatma metinlerinin acente sıfatı ile bankalar tarafından kişisel veri elde edilmesi esnasında sigorta şirketi adına müşterilere teslim edilmesi/İnternet şube kanalı ile poliçe satışının söz konusu olduğu durumlarda yine veri sorumlusu sigorta şirketi tarafından hazırlanan aydınlatma metinlerinin internet şube kanalı ile sigorta müşterilerine okutulması),
- Veri sorumlusu adına veri işleyen tarafından ilgili kişilerin açık rızasının alınması halinde veri işleyenin yükümlülükleri, (örnek olarak, sigorta şirketi tarafından açık rızaya tâbi bir veri işleme faaliyeti gerçekleştiriliyor ise bankadan sigorta poliçesi talebinde bulunan ilgili kişilerden talep edilecek açık rıza beyanlarının sigorta şirketinin belirleyeceği usul ve esaslar kapsamında banka tarafından alınması),
- Tarafların birbirlerini bilgilendirme ve iş birliğinde bulunma yükümlülüğü, (örnek olarak kişisel veri ihlali yaşanması veya silmenin gerçekleştirildiğine dair rapor sunulması),
- Taraflar arasındaki sorumluluğun tespiti, sınırlandırılması ve rücu ilişkisi.

Bunların dışında, Kanuna ve somut olaya uygun olduğu ölçüde, veri işleme ve alt veri işleme faaliyetleri yönünden, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından düzenlenen Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik'in" "Destek Hizmeti Alınması" başlıklı ikinci bölümünün "Destek hizmeti kuruluşlarında aranacak şartlar" başlıklı 6 ncı ve "Sözleşmenin Unsurları" başlıklı 7 nci maddelerindeki destek hizmeti firmaları ve alt yüklenicilere ilişkin hükümlerden yararlanılabilir. Banka ile destek hizmeti kuruluşları arasında akdedilecek sözleşmeler hem Kanun hem Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik hükümlerine uygun şekilde düzenlenmelidir.

2. Destek Hizmetleri

Destek hizmeti kuruluşu, 5411 sayılı Kanun'un "Tanımlar ve Kısaltmalar" başlıklı 3 üncü maddesinde "Bankaların, mevduat veya katılım fonu kabulü, nakdi, gayrinakdi her cins ve surette kredi verme ve bu Kanunun uygulamasında kredi olarak sayılan işlemler dışında kalan faaliyetlerini banka adına gerçekleştiren; ya da reklamının yapılması hariç olmak üzere mevduat veya katılım fonu kabulü dışındaki faaliyetlerinden herhangi birinin pazarlanması da dâhil gerçekleştirilmesinde bankaya yardımcı nitelikte hizmet veren kuruluşlar" şeklinde tanımlanmıştır.

Bu durumda destek hizmeti kuruluşlarının veri sorumlusu veya veri işleyen sıfatlarından hangisini haiz oldukları her veri işleme faaliyeti bakımından somut olayın özelliklerine göre değerlendirilmelidir. Örneğin kurye, kargo firması gibi şirketlerin teslim etmesi gereken kredi kartı, ekstre gibi kişisel veri niteliğindeki müşteri sırrı içeren belgelerin içeriğine yönelik veri işleme faaliyeti gerçekleştirmedikleri açıktır. Ancak teslime yönelik, banka tarafından bahsi geçen şirketlere aktarılan bilgilerin (isim, soy isim, telefon, adres vb. işin niteliği gereği aktarılan bilgiler) nasıl kullanılacağına bu şirketlerce tâbi oldukları yasal düzenlemeler göz önüne alınarak karar verilmektedir. Bu nedenle aktarılan bilgiler yönünden kargo ve kurye şirketleri gibi firmalar da veri sorumlusu sıfatını haizdir.

Ancak bu durumda dahi kargo ve kurye şirketleri gibi firmaların kişisel veri içeren belgenin doğru kişiye teslim edilmesi veya kaybolmaması için veri güvenliği yönünden sorumlulukları bulunmaktadır. Dolayısıyla bu şirketlerin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak başta olmak üzere Kanundan doğan yükümlülüklerini yerine getirmesi gerekmektedir.

Uygulamada bankalarca veri işleyen konumunda bulunan ve tüm hizmet alınan şirketlere aktarılan verilerin, bu şirketlerce kendisine menfaat sağlayacak şekilde kullanıldığı durumlar mevcuttur. Veri işleyenin edindiği

verileri kendi adına kullanması durumunda veri işleyen o kişisel veri işleme faaliyeti bakımından veri sorumlusu gibi sorumlu olacaktır.

3. İştirakler ve Bağlı Ortaklıklar

Bankalar aynı zamanda BDDK'nın faaliyet genişlemesi iznine istinaden bağlı ortaklıklarına hizmet verebilmektedirler. Bu hizmetler yönünden verilen her hizmete özelinde değerlendirme yapılmalı ve tarafların veri sorumlusu-veri işleyen sıfatları yukarıdaki kıstaslar da uygulanarak belirlenmelidir.

Örnek vermek gerekirse Türkiye'de bulunan banka, yurtdışında yerleşik bağlı ortaklığının kredi sözleşmesinin imzalarının teminine yönelik hizmet vermesi halinde, veri işleyen sıfatını haiz olacaktır. Bu noktada, bankaların sağlayacakları hizmetin niteliğine göre veri sorumlusu-veri işleyen sıfatını almaları mümkün olabilecektir. Bir başka deyişle, sıfatın tespiti, kişisel veri işleme faaliyetinin niteliğine göre her somut olay bakımından ayrıca değerlendirilmelidir.

4. Açık Bankacılık

Açık Bankacılık servisleri, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'in "Tanımlar ve kısaltmalar" başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde "Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalı" şeklinde tanımlanmıştır. Açık bankacılık hizmetlerinde, üç temel işleme faaliyetinin bulunduğundan bahsedilebilir[7]:

1) Gerçek kişi müşterinin kişisel verilerinin bankacılık hizmetlerinin sunulması amacıyla banka tarafından işlenmesi: Bu işleme faaliyeti,

[7] Taştan, Furkan Güven/Saruhan, Utku (2020) Açık Bankacılık: Kişisel Verilerin Korunmasına Bir Tehdit Mi? (Çevrimiçi Yayın) https://www.researchgate.net/publication/345514465_Acik_ Bankacilik_Kisisel_Verilerin_Korunmasina_Bir_Tehdit_Mi (Son Erişim Tarihi: 29.07.2022).

gerçek kişinin bankayla hukuki ilişkisinin kurulmasıyla başlamakta olup müşterinin kimlik bilgilerinden, işlem güvenlik bilgilerine ve işlem geçmişine ilişkin çok çeşitli finansal ve diğer kişisel verileri içermekte olup şüphesiz ki burada veri sorumlusu bankadır.

2) Gerçek kişi müşterinin kişisel verilerinin açık bankacılık ürün ve hizmetlerinden faydalandırılması amacıyla üçüncü taraf sağlayıcı tarafından işlenmesi: Burada müşterinin API aracılığıyla üçüncü taraf sağlayıcıya aktarılan kişisel verileri, ürün ve hizmetlerin kendisine sunulması amacıyla işlenmektedir. Örneğin bir müşterinin birden çok bankada bulunan bakiye hesap ve işlem geçmişi bilgilerinin, müşteriye yatırım veya harcama tavsiyelerinde bulunması amacıyla üçüncü taraf sağlayıcı tarafından kendi özel algoritmalarıyla işlenmesi halinde üçüncü tarafın da veri sorumlusu olduğu açıktır. API bakımından da veri sorumluluğu değerlendirilebilir.

3) Gerçek kişi müşterinin belirli kategorilerdeki kişisel verilerinin banka tarafından üçüncü taraf sağlayıcıya aktarımı ve bununla eş zamanlı olarak üçüncü taraf sağlayıcının bu verileri kendi veri kayıt sistemine kaydetmesi: Bu işleme faaliyetinde banka örneğin API aracılığıyla kendi veri kayıt sisteminden üçüncü taraf sağlayıcıya gönderilmek üzere veri aktarımında bulunmaktadır. Üçüncü taraf sağlayıcı da bu API aracılığıyla verileri kendi veri kayıt sistemine çekmektedir. Bu faaliyet bakımından gerek kişisel verileri aktaran tarafın gerek kişisel verileri kendi sistemine kaydeden tarafın veri sorumlusu sıfatını haiz olması mümkündür.

5. Bankaların Acente Sıfatıyla Hareket Ettiği Durumlar

5411 sayılı Kanun'un "Faaliyet konusu" başlıklı 4 üncü maddesinin (u) bendi uyarınca bankalar sigorta acenteliği ve bireysel emeklilik aracılık hizmetlerini gerçekleştirmeye yetkilidir.

5684 sayılı Sigortacılık Kanunu'nun "Sigorta acenteleri" başlıklı 23 üncü maddesi ve Sigorta Acenteleri Yönetmeliği'nin "Bankalar ve özel kanunlarına

istinaden acentelik yapan kurumlar" başlıklı 13 üncü maddesi bankaların acente sıfatıyla sigortacılık faaliyeti göstermelerine ilişkin hususları düzenlemektedir.

Bankaların, düzenlenen bir sektör olan sigorta sektöründe ilgili yasal düzenlemeler uyarınca acente sıfatıyla yerine getirdikleri sigortacılık faaliyetleri bakımından veri işleyen veya veri sorumlusu sıfatından hangisini haiz olduğunun tespiti önemlidir. "Veri sorumlusu" kişisel verilerin işlenme amaçlarını, vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. 5684 sayılı Kanunun "Tanımlar" başlıklı 2 nci maddesinin (m) bendinde sigorta acenteleri, "sigorta şirketlerinin nam ve hesabına sigorta sözleşmelerine aracılık eden, sözleşme akdinden önce hazırlık çalışmalarını yürüten veya sözleşmenin uygulanması ile tazminat ödenmesinde yardımcı olan" kişi olarak tanımlanmaktadır. Bu doğrultuda, bankaların acente sıfatıyla yaptıkları sigortacılık faaliyetlerinde hangi kişisel verilerin hangi amaçla işleneceğine, kişisel veri işleme faaliyetinin hangi vasıtalarla işleneceğine bankalar karar vermediğinde ve veri kayıt sisteminin kurulmasının ve yönetilmesinin sorumluluğunun sigorta şirketlerinde bulunduğu sigortacılık faaliyetlerinde bankalar, veri işleyen sıfatını haizdir.

Bankalar veri işleyen sıfatını haiz oldukları kişisel veri işleme faaliyetleri bakımından da Kanun kapsamındaki veri güvenliğine ilişkin yükümlülüklerini yerine getirmelidir. Öte yandan, bankaların veri işleyen sıfatını haiz olduğu kişisel veri işleme faaliyetleri bakımından Kanunun 10 uncu maddesi uyarınca aydınlatma yükümlülüğünün yerine getirilmesinden ve açık rıza ile kişisel veri işleme faaliyetinin gerçekleştirileceği durumlarda ilgili kişilerin açık rızalarının alınmasından sorumlu tutulmaları, ancak veri sorumlusu tarafından bu hususlarda görevlendirilmiş olmaları halinde mümkündür.

V. İlgili Kişi

İlgili kişi, Kanunun 3 üncü maddesinde kişisel verisi işlenen gerçek kişi olarak tanımlanmıştır. Bankacılık sektöründe ilgili kişi kategorisine giren kişiler çeşitlidir. Çalışan adayı, çalışan, çalışan eş ve çocukları, stajyer, tedarikçi çalışanı, müşteri, ziyaretçi, kefil, veli/vasi/temsilci gibi pek çok kişinin kişisel verileri işlenebilmektedir.

Bu kapsamda rehberde kişisel verisi işlenen ilgili kişilere konuya ve ilgisine göre yer yer değinilmiştir.

VI. İşlenen Kişisel Veriler

Bankacılık sektöründe işlenen kişisel veriler özel nitelikli kişisel verileri de içerebilmektedir. Bu kapsamda kategorik bazda kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama, görsel ve işitsel kayıtlar gibi kişisel verilerin yanı sıra ceza mahkumiyeti ve güvenlik tedbirleri, biyometrik veri ve sağlık bilgileri gibi özel nitelikli kişisel veri türleri de işlenebilmektedir.

VII. Kişisel Veri İşleme Şartları

6698 sayılı Kanunun 5 inci maddesinde kişisel verilerin işlenmesinin hangi şartlarda mümkün olduğu düzenlenmiştir:

- Açık rızanın bulunması.
- Kanunlarda açıkça öngörülmesi.
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel verilerin işlenme şartları, yani hukuka uygunluk halleri, Kanunda sayma yoluyla belirlenmiş olup bu şartlar genişletilemez[8]. Veri sorumlusu tarafından kişisel veri işleme faaliyetinin amacının öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli; eğer bu amaç Kanunda belirtilen açık rıza dışındaki şartlardan en az birini karşılamıyorsa bu durumda veri işleme faaliyetinin devamı için Kanunun 4 üncü maddesinde hükme bağlanan genel ilkeler de dikkate alınmak suretiyle kişinin açık rızasının alınması yoluna gidilmelidir[9]. Bankacılık faaliyetlerinin kapsamı ve sınırları ilgili mevzuat düzenlemelerinde kesin bir şekilde belirlenmiş olduğundan esasen bankalarca yapılan veri

[8] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s.2.
[9] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s.3.

işleme uygulamaları büyük ölçüde açık rıza dışındaki hukuka uygunluk nedenlerine dayanmaktadır. Her bir veri kategorisi, birden fazla amaçla işlenerek işlendikleri amaca göre farklı hukuka uygunluk nedenlerine tabi olabilecekleri gibi bir işleme amacı birden fazla hukuka uygunluk nedenine de dahil olabilmektedir.

Örneğin, 6362 sayılı Sermaye Piyasası Kanunu'nun 57 nci maddesinin 3 üncü fıkrasında "Konut finansmanı kuruluşları tarafından, konut edinme amacının yeterli bilgi ve belgeyle tespit edilmesi ve kullandırılan kredinin veya yapılan finansal kiralamanın ipotek veya Kurulca uygun görülen teminatlar ile güvence altına alınması zorunludur." hükmüne yer verilmiştir.

Bu çerçevede, kredinin teminatla güvence altına alınması kanunen zorunlu olup bu durum aynı zamanda Konut Finansmanı Kredisi Sözleşmesi'nde de düzenlendiğinden, ipotek alınması amacıyla işlenen söz konusu kişisel veriler yönünden hem Kanunun 5 inci maddesinin 2 nci fıkrasının (a) bendinde yer alan kanunlarda açıkça öngörülmesi hem de (c) bendinde yer alan bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması nedeniyle, ilgili kişilerin açık rızalarına başvurulmasına gerek bulunmayabilecektir.

1. Açık Rıza

6698 sayılı Kanunun 3 üncü maddesinde açık rıza; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlanmıştır. Açık rızanın bu anlamda, rıza veren kişinin olumlu iradesini göstermesi gerekmektedir[10].

Kanunun 5 inci maddesi uyarınca açık rıza Kanundaki kişisel veri işleme şartlarından biridir ve diğer kişisel veri işleme şartlarına göre karşılaştırmalı bir üstünlüğü bulunmamaktadır.

[10] Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi, s.3.; "Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünü usulüne uygun yerine getirmediği iddiaları hakkında" Kişisel Verileri Koruma Kurulunun 08/07/2019 tarih ve 2019/206 sayılı Karar Özeti, www.kvkk.gov.tr

Kanun'da açık rızanın alınmasına ilişkin herhangi bir şekil şartı öngörülmemektedir. Kişilerin rızalarının "açık" olması, bu rızanın mutlaka yazılı olarak ortaya konmuş olması anlamını taşımamaktadır[11]. Herhangi bir metne bağlı olmasa dahi iki taraf arasında işleyen süreç ve karşılıklı eylemler açık bir rızanın varlığına işaret edebilir.

Örneğin, 5378 sayılı Engelliler Hakkında Kanunun 7 nci maddesi ve "Bankacılık Hizmetlerinin Erişilebilirliğine Dair Yönetmelik"in 4 üncü maddesinin sekizinci ve dokuzuncu fıkraları uyarınca, %40 ve üzeri oranda engelli olduğuna ilişkin belgenin aslını veya banka tarafından onaylanacak suretini müşterisi olduğu bankaya ibraz eden ayırt etme gücüne sahip kişilerin engelli kabul edilerek, Yönetmelikte tanınan haklardan yararlanacağı hüküm altına alınmıştır. Söz konusu düzenleme uyarınca bankaların, bu kapsamda belge ileten engelli müşterilerin engel durumuna ilişkin bilgi ve belgeleri tutma yükümlülüğü bulunmaktadır.

Bununla birlikte, 6698 sayılı Kanunun 6 ncı maddesi uyarınca anılan Yönetmelik kapsamında engellilik durumunun bankalarca kayıt altına alınması özel nitelikli kişisel verilerin işlenmesi olarak değerlendirilebilecektir. Özel nitelikli kişisel verilerin işlenmesi bu rehberin "Bankalarca işlenen Özel Nitelikli Kişisel Veriler" başlığı altında detaylı olarak açıklanmaktadır.

Kanunda açık rıza alınmasının şekil şartı belirlenmediğinden, ilgili kişi tarafından anılan Yönetmelik kapsamındaki erişilebilirlik imkanlarından faydalanmak üzere bu konudaki niyetinin açık şekilde ortaya koyulması suretiyle bankaya talepte bulunulması, duruma göre açık rızanın ortaya konulması olarak değerlendirilebilir. Bu kapsamda söz konusu talebin açık rıza teşkil etmesi için ilgili kişinin kişisel verilerinin işlenmesi hususunda banka tarafından aydınlatma yükümlülüğünün de yerine getirilmesi gerekmektedir. Zira açık rızanın özgür irade dışındaki diğer unsurları belirli bir konuya ilişkin olması ve bilgilendirmeye dayanmasıdır ve aydınlatma suretiyle bu unsurların da karşılanması mümkün olabilecektir.

[11] Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi, s.3.

Benzer şekilde, bankanın internet sitesindeki talep ve şikâyet bölümüne kendi isteğiyle hastalık detaylarından bahseden bir gerçek kişinin bu bilgilerinin ilgili süreci yürütmek amacıyla Kanunun 4 üncü maddesindeki genel ilkeler çerçevesinde bankaca işlenebileceğine dair açık rızasını ortaya koyduğu kabul edilebilir.

1.1. Açık Rızanın Unsurları

1.1.1. Belirli Bir Konuya İlişkin Olma

Veri işlemek üzere verilen rızanın geçerli olması için rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması gerekir.

Eğer birden çok kategoriye ilişkin verinin işlenmesine dair açık rıza beyanında bulunulacaksa açık rızanın, hangi verilerin ve ne amaçlarla işleneceği gibi işlemenin farklı noktaları açısından da verilmiş olması gerekir.

1.1.2. Özgür İradeyle Açıklanmış Olma

Açık rıza ilgili kişinin özgür iradesiyle açıklanmış olmalıdır. İlgili kişinin irade beyanı olan rıza, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacaktır.

Öte yandan açık rızanın özgür irade ile açıklanması gerektiğinden ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir[12]. Örneğin müşteri ve hesap açılış işlemleri sırasında, pazarlamaya ilişkin açık rıza vermeyen müşterilerin de müşteri ve hesap açılış işlemleri gerçekleştirilmelidir.

[12] "Hizmetin Açık Rıza Şartına Bağlanması" konulu Kişisel Verileri Koruma Kurulu Kararı; Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti; "İlgili kişinin araç kiralama hizmeti alması esnasında kişisel verilerinin işlenmesine dair açık rıza vermemesi üzerine kiralama hizmetinden yararlandırılmaması"na ilişkin Kişisel Verileri Koruma Kurulu'nun 05/05/2020 tarihli ve 2020/335 sayılı Karar Özeti, www.kvkk.gov.tr

1.1.3. Bilgilendirmeye Dayanma

Açık rızaya başvurulmadan önce ilgili kişinin açık rızaya dayalı kişisel veri işleme faaliyetine yönelik olarak bilgilendirilmesi gerekir. Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirildiği durumlarda, aydınlatma yükümlülüğünün ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.

1.2. Kanala Özgü İyi Uygulama Örnekleri

İlgili kişilerden alınacak olan açık rızanın "yazılı olma" koşulu bulunmadığı için bankanın ıslak imzalı ve yazılı bir metin temin etme zorunluluğu bulunmamakla birlikte açık rıza alındığının ispat yükümlülüğü veri sorumlusu bankadadır. İspatın sağlanması açısından "kalıcı veri saklayıcısı"[13] olarak kabul edilen araç ve yöntemler aracılığı ile açık rızanın alınmasının ispat hususunda bankaların kullanabileceği elverişli yöntemleri içermektedir[14]. Böylelikle bankacılık uygulamalarında şube, ATM, internet şubesi, çağrı merkezi, mobil uygulama gibi benzer mecralar aracılığıyla kişinin açık rızası alınabilir.

Örneğin ilgili kişilerin internet ve mobil bankacılık kanalından yaptığı işlemlerde şifre/parola girilmesiyle kimlik tespiti sağlanabildiği ve kişilerin yaptığı işlemlerin kayıt altında tutulabildiği bu kanallar da ispata elverişli bir alandır.

Diğer bir örnek olarak; bankanın internet sitesine girerek kredi başvurusunda bulunan bir kişiye kredi kullandırılması faaliyetine özel aydınlatma yapıldıktan sonra pazarlama amacına yönelik olarak açık rızası alınması suretiyle beyan etmiş olduğu iletişim bilgisine sms/e-posta vb. ile doğrulama yapılarak açık rızasının alındığı hususu ispata elverişli hale getirilerek, pazarlama faaliyetleri için kişisel verileri işlenebilir.

[13] TKHK'nun 3'ncü maddesinin (f) bendi ile Finansal Hizmetlere İlişkin Mesafeli Sözleşmeler Yönetmeliği'nin 4'ncü maddesinin (c) bendi kapsamında kalıcı veri saklayıcısı tanımına yer verilmiştir.

[14] Ozcan, Göknil, Bankacılık İş Ve İşlemlerinde Kişisel Verilerin Korunması, On İki Levha Yayıncılık, 1. Baskı, Ocak 2020, s. 57

1.2.1. Şube

Şube kanalı ile ilgili kişilerden, ıslak imza veya onun yerini tutacak mevzuatın öngördüğü diğer yöntemlerle (dijital imza, e-imza vb.) açık rıza metinleri için onay alınabilir.

1.2.2. ATM

ATM'den ilgili kişilerden açık rıza alınmak istendiği takdirde ilgili kişinin söz konusu kanallara girişi sonrasında açık rıza metni için onayı alınabilecektir.

1.2.3. İnternet/Mobil Bankacılık

İnternet bankacılığı/mobil bankacılık kanallarında ilgili kişilerden açık rıza metinlerine onay alınması için kişilerin işaretleyebileceği kutu/buton vb. yöntemler kullanılabilmektedir. Bu kutu/buton vb. yöntemler ile gerçekleştirilen seçimlerde seçeneklerin önceden seçili olarak getirilmemesi gerekir.

1.2.4. Çağrı Merkezi

Çağrı merkezinde, ilgili kişilere görüşmede tercihini bir tuşa basma veya müşteri temsilcisine sözlü olarak beyan etme imkânı sağlanarak açık rıza onayı alınabilir.

1.2.5. SMS

İlgili kişilerin bankada kayıtlı olan telefon numaralarına SMS aracılığı ile aydınlatma yapılarak ve SMS aracılığı ile doğrulama kodu gönderilerek kişisel verilerinin işlenmesi konusunda bir cevap vermesi yönünde yönlendirme yapılabilir.

Kurum tarafından yapılan kamuoyu duyurusunda da belirtildiği üzere bankalarca ilgili kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar

doğuracağı hususları ilgili kişiye bildirilmelidir. Katmanlı aydınlatmanın bir gereği olarak SMS içeriklerinde aydınlatma yükümlülüğünün yerine getirilmesini sağlayacak gerekli kanallar sağlanmalıdır[15].

1.2.6. Elektronik Posta

İlgili kişilerin bankada kayıtlı elektronik posta adresine, aydınlatma ve açık rıza metinleri yönlendirilebilecek, bu kanalda ilgili kişilerden açık rıza metnini kabul edip etmediği yönünde beyanını yöneltmesi için kutular sunulabilecektir.

2. Kanunlarda Öngörülmesi ve Hukuki Yükümlülüğün Yerine Getirilmesi

Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde geçen "kanunlarda açıkça öngörülmesi" ifadesi ile kişisel verilerin işlenmesiyle ilgili herhangi bir kanunun kast edildiği anlaşılmaktadır. Anılan hükmün (ç) fıkrası uyarınca ise veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlenmesinin zorunlu olduğu hallerde ilgili kişinin kişisel verileri işlemesi mümkündür.

Bu kapsamda, her iki şarttan birinin mevcut olduğu durumlarda kişisel veri işleme faaliyetleri için açık rıza alınmamalıdır[16]. Kişisel veri işlenmesiyle ilgili herhangi bir kanunda açık bir hüküm varsa veya açık bir hüküm ile ikincil mevzuata yönlendirme yapılmışsa bu durumda kişisel verilerin işlenmesi mümkündür[17]. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlenmesinin zorunlu olduğu hallerde ise kanun veya

[15] KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu, (Çevrimiçi), 04.04.2022.

[16] "İlgili kişinin bir kargo şirketine karşı açtığı işe iade davasında, kişisel verisi olan kamera görüntülerinin kargo şirketi tarafından mahkemeye sunulması" hakkında Kişisel Verileri Koruma Kurulunun 25/06/2020 tarihli ve 2020/494 sayılı Karar Özeti; "Avukatların icra takip dosyalarındaki kişisel verilere vekâletname olmaksızın hukuka aykırı olarak erişim sağladığına ve Adalet Bakanlığı tarafından icra tevzi bürolarında görevli personel eliyle alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılmasına ilişkin ihbarlar hakkında" Kişisel Verileri Koruma Kurulunun 20/05/2021 tarihli ve 2021/511-512-513 sayılı Karar Özeti, www.kvkk.gov.tr

[17] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s.6.

ikincil mevzuatta veri sorumlusuna getirilen hukuki yükümlülüğün yerine getirilmesinin kişisel veri işlemeyi zorunlu kılması söz konusudur.

Bankaların kredilendirme işlemleri öncesinde kredi başvurusunda bulunanlar için risk grubu bazında risklilik değerlendirmesinde bulunması, 5411 sayılı Bankacılık Kanunu'nun 49 uncu maddesi vd. ile Bankaların Kredi İşlemlerine İlişkin Yönetmelik uyarınca hukuki bir yükümlülüktür. Bu kapsamda, kredi başvurusunda bulunanların risk değerlendirme sürecine giren her türlü kişisel veri belirtilen amaçla açık rıza alınmaksızın işlenebilecektir.

Bunlarla sınırlı olmamakla birlikte:

- 5411 sayılı Bankacılık Kanunu ve ikincil mevzuat uyarınca BDDK veya bağımsız danışmanlık ve denetim şirketleri tarafından bankacılık sektörüne özgü, finansal veya güvenlik amacıyla gerçekleştirilen denetimlerde bankalarca bilgi paylaşımında bulunulması,
- İlgili düzenlemelerin ne şekilde uygulanması gerektiğine dair ilgili kurumların (T.C. Gümrük ve Ticaret Bakanlığı, Mali Suçları Araştırma Kurumu, Gelir idaresi Başkanlığı gibi) başvuruda bulunan bankalara veya Türkiye Bankalar Birliği'ne/Türkiye Katılım Bankaları Birliği'ne üyelerine duyurulmak üzere gönderdikleri yol gösterici yazı ve kararları çerçevesinde kişisel verilerin işlenmesi,
- Suç Gelirlerinin Aklanmasının Önlenmesine ilişkin ilgili mevzuat uyarınca bankaların yapılan işlemler bazında gerçek kişilere ilişkin olarak kimlik tespiti yükümlülüğünün olması ve bu yükümlülüğün yerine getirildiğini ispat amacıyla yapılan işlemler,
- 5941 sayılı Çek Kanunu'nun 2 nci maddesinin ikinci fıkrası uyarınca, çek karnesi tahsis sürecinde çek karnesi talebinde bulunan ilgili kişinin çek yasaklısı olup olmadığının tespitine yönelik adli sicil kaydı sorgusu yapılması,

açık rıza alınmasını gerektirmeyen durumlar arasındadır.

2.1. Bankaların Tabi Olduğu Mevzuata İlişkin Yükümlülüklerinin Değerlendirilmesi

2.1.1. Mevzuat

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 5'nci maddesinin 2'nci fıkrasının (a) bendinde kanunlarda açıkça öngörülen durumlarda ilgili kişinin açık rızası alınmaksızın kişisel verilerin işlenebileceği düzenlenmiştir. Kanun'un 5'inci maddesinin 2'nci fıkrasının (ç) bendinde ise veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması durumunun da veri işleme için ilgili kişiden açık rıza alınmasına gerek olmayan hallerden sayılacağı belirtilmektedir.[18] Bir işleme faaliyeti sayılan müşteri bilgisinin ifşası/açıklanması ise 5411 sayılı Bankacılık Kanunu'nun 73'üncü maddesi altında düzenleme altına alınmış olup, bu düzenleme içeriğinde Kanun ile paralel olarak banka müşterilerine ait sırları öğrenenlerin, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamayacakları ve Bankacılık Kanunu'nda belirtilen haller harici üçüncü kişilere ifşa edemeyecekleri belirtilmektedir.

2.1.2. Bankacılık Faaliyetleri Kapsamında Kanunlarda Öngörülen İşlemeler

Aşağıda sayılan Kanun maddeleri ile sınırlı olmamakla birlikte, bankaların gerçekleştirdiği faaliyetler çerçevesinde kanunlarda açıkça öngörülen ve ilgili kişiden açık rıza alınmasına gerek olmayan haller kapsamında

[18] Hukuki yükümlülüğün yerine getirilmesi işleme şartı kapsamında bkz. "İlgili kişilerin kişisel verileri olan banka hesap hareketlerinin, mevduat bilgilerinin, para yatırma ve çekme işlemlerinin açık rızaları olmaksızın vergi müfettiş yardımcısı tarafından hukuka aykırı olarak işlenmesi hakkında" Kişisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/120 sayılı Karar Özeti; "İlgili kişinin, veri sorumlusu bir banka nezdindeki kişisel verileri olan hesap ve kiralık kasa bilgilerinin aktarılması hakkında" Kişisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/118 sayılı Karar Özeti; "Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında" Kişisel Verileri Koruma Kurulunun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti; "Veri sorumlusu hastanede uygulanan beyaz kod kapsamında ilgili kişinin işlenen kişisel verileri hakkında" Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/63 sayılı Karar Özeti; "Veri sorumlusu sağlık firması tarafından eski çalışanı olan ilgili kişinin kişisel verilerinin rızası alınmaksızın aktarım hakkında" Kişisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı Karar Özeti, www.kvkk.gov.tr

değerlendirilebilecek veri işleme örnekleri aşağıda sayılmaktadır:

2.1.2.1. Bankacılık Kanunu Madde 73 ve Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik

5411 sayılı Bankacılık Kanunu'nun 73'üncü maddesi sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenlerin söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamayacağı hüküm altına alınmış olmakla birlikte aynı maddenin 4'üncü fıkrasında hangi hallerde bir işleme sayılan müşteri/banka sırrı paylaşımı ve ifşasının bu kuralın istisnası olarak değerlendirileceği düzenleme altına alınmıştır.

Söz konusu maddeler dahilinde aşağıda sayılan paylaşım/ifşalar Kanun kapsamında ilgili kişinin açık rızası alınmaksızın gerçekleştirilebilecektir. Bankacılık Kanunu'nun anılan maddesi kapsamında belirtilen sır saklama yükümlülüğünden istisna tutulan hallerde yapılacak paylaşımlar da dahil olmak üzere, yapılan paylaşım/ifşaların belirtilen amaçlarla sınırlı ve ölçülülük ilkesine uygun ve amacın gerektirdiği kadar veriyi içermek kaydıyla yapılabileceği düzenlenmiştir.

Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik[19] 5'inci maddesinde de sır saklama yükümlülüğünden istisna tutulan haller düzenlenmiştir.

Bankacılık Kanunu ve Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik düzenlemeleri çerçevesinde;

- Kanunen yetkili kılınan bir adli ya da idari kurumun ya da kişinin talebi üzerine bu kurum ve kişiler ile yapılacak veri paylaşımları
- Gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla;

  a) Bankaların ve finansal kuruluşların, kendi aralarında

[19] 04.06.2021 tarih, 31501 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik

doğrudan doğruya ya da Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla her türlü bilgi ve belge alışverişinde bulunması.

b) Konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları kapsamında bankaların sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıklarına bilgi ve belge verilmesi.

c) Doğrudan veya dolaylı pay sahipliği yoluyla banka sermayesinin yüzde onunu ve daha fazlasını temsil eden payların satışı amacıyla yapılacak değerleme çalışmalarında kullanılmak üzere muhtemel alıcılara bilgi ve belge verilmesi veya krediler dâhil varlıkların ya da bu varlıklara dayalı menkul kıymetlerin satışı amacıyla yapılacak değerleme çalışmalarında kullanılmak üzere bilgi ve belge verilmesi.

ç) Değerleme, derecelendirme, destek hizmeti ile bağımsız denetim faaliyetlerinde veya gerekli teknik ve idari tedbirlerin alınması kaydıyla hizmet alımlarına yönelik işlemlerde kullanılmak üzere bu hizmeti sağlayanlara bilgi ve belge verilmesi.

- Konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları kapsamında bankaların sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıklarına bilgi ve belge verilmesi amacıyla yapılacak İSEDES Yönetmeliğinde[20] yer verilen risk yönetim sistemi içinde yer alan uyum, kredi, itibar riskleri de dâhil olmak üzere tüm risk kategorilerine ilişkin risk yönetim faaliyetlerini kapsayacak şekildeki paylaşımların, bu amaçlar ile sınırlı kılınması, gizlilik sözleşmesi yapılması, söz konusu sözleşme hükümleri ile karşı tarafın gerekli teknik ve idari tedbirleri almasının sağlanması koşuluyla, hakim ortak ile yapılması ya da hakim ortağın/ana ortaklığın belirleyeceği, konsolide finansal tablo hazırlama ya da

[20] 11.07.2014 tarih, 29057 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik.

konsolide risk yönetimi uygulamaları kapsamında hizmet aldığı bir grup şirketi ile yapılması,

- Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulmuş şirketlerce, müşterilerin kamu kurum ve kuruluşlarına kendi talepleri ile verdikleri müşteri sırrı niteliğindeki bilgilerin teyit edilmesi konusunda müşteri talep ya da talimatının alınmış olması şartıyla, söz konusu kamu kurum ve kuruluşlarına bu bilgilerin sadece doğru olup olmadığı şeklinde cevap verilmesi,
- Bankanın taraf olduğu uyuşmazlıklarda iddia ya da savunmasının ispatı için zorunlu olması halinde, söz konusu uyuşmazlığın tarafı olan gerçek veya tüzel kişilere ait müşteri sırrı niteliğindeki bilgilere veya banka sırrı niteliğindeki bilgilere ilişkin olarak, yurt içindeki ya da yurt dışındaki yargı makamları ile tahkim, arabuluculuk ve hakem heyeti gibi alternatif uyuşmazlık çözmeye yetkili makamlarla ya da bu makamlarla paylaşmak üzere söz konusu uyuşmazlıklarda bankayı temsil eden taraflarla yapılan paylaşımlar,
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un[21] 5. maddesi uyarınca finansal gruba bağlı kuruluşların, müşterinin tanınmasıyla hesap ve işlemlere ilişkin olarak grup içerisinde bilgi paylaşımı,
- Kişisel Verileri Koruma Kurulu'nun Bankacılık Kanunu'nun 73'üncü maddesi kapsamında yapılacak paylaşımlara yönelik Türkiye Bankalar Birliği muhatap 07.08.2020 tarih, 67322700-045.02-E.0000029767 sayılı yazısında esasen kişisel verilerin bankacılık hukukunda özel bir görünümü olan gerçek kişi müşteri sırları (müşteri bilgileri) bakımından 5411 sayılı Kanun'un hükümleri, 6698 sayılı Kanun'a göre özel hüküm niteliğini haiz bulunduğu; özel norm-genel norm ilişkisinde özel normların uygulama alanı bulacağı değerlendirmesinde bulunulmuştur.[22] Bu kapsamda, Bankacılık Kanunu tahtında müşteri bilgilerinin Bankacılık Kanunu'nun 73 üncü maddesine dayalı olarak yapılacak paylaşımlara genel norm-özel norm prensipleri çerçevesinde Bankacılık Kanunu'nun uygulanacağı;

[21] 18.10.2006 tarih, 26323 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun

[22] Kişisel Verileri Koruma Kurumu'nun 07.08.2020 tarih, 67322700-045.02-E.0000029767 sayılı yazısı.

Kişisel Verilerin Korunması Kanunu hükümlerinin uygulanmayacağı söylenebilecektir.

2.1.2.2. Risk Değerlendirmesi

Bankalar, faaliyetleri çerçevesinde kredi riski, piyasa riski ve operasyonel risk ana başlıkları altında ele alınan genel, sektörel ve mikro bazda risklerle karşılaşmaktadır. Kredi riski, kredi borçlusunun anapara veya faiz ödemeleri ile ilgili yükümlülüklerini zamanında veya tam olarak yerine getirememesi nedeni ile bankaların maruz kaldığı en temel risklerin başında gelmektedir. Bankacılıkta risk yönetiminin önemli ilkelerinden biri, üstlenilen risk sonucu oluşabilecek zarar ihtimaline karşı kaynak ayrılması, başka bir deyiş ile sermaye tahsis edilmesidir.

Bankacılıkta; üstlenilen risk, tahsis edilen sermaye ve beklenen getiri arasında pozitif bir ilişki bulunmaktadır. Bu üç olgu arasında üstlenilen riskler özel bir önem içermekte; riskin doğru ölçülmesi, tahsis edilecek sermaye tutarını da doğrudan etkilemektedir.

Bankaların finansal risklerinin yönetilmesi kapsamında, müşteri veya müşteri adaylarına yönelik analiz yapmak ve müşterilerin kredi başvuruları sonrasında, kredilendirme sürecinde yasal sınırları dikkate alma zorunluluğu bulunmaktadır. Kişisel Verileri Koruma Kurulu'nun (Kurul) 26/07/2018 tarihli ve 2018/92 sayılı kararı ile, 5411 sayılı Bankacılık Kanunu'nun 49'uncu maddesi ve ilgili diğer mevzuat hükümleri çerçevesinde bankalar tarafından "risk grubu" içerisinde yer alanların kişisel verilerinin işlenmesinin, 6698 sayılı Kanunun 5'inci maddesinin ikinci fıkrasının (ç) bendi uyarınca bankaların hukuki yükümlülüklerinin yerine getirilmesi kapsamında olduğu kanaatine varılmıştır.

Yine Kişisel Verileri Koruma Kurulu, risk grubunun 5411 sayılı Bankacılık Kanununda tanımlandığı, 5411 sayılı Bankacılık Kanunu ve ilgili diğer mevzuat hükümleri çerçevesinde "Risk Grubu" içerisinde yer alan kişilerin kişisel verilerinin, ancak bankacılık faaliyetleri kapsamında, kendi bankası bünyesinde kullanılmak ve Risk Merkezine aktarılmak amacıyla işlenmesinin,

6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin ikinci fıkrasının (ç) bendi uyarınca bankaların hukuki yükümlülüklerinin yerine getirilmesi kapsamında olduğunun değerlendirilmesi gerektiği değerlendirmesinde bulunmuştur.[23]

Bu kapsamda, kredi kullandırılan gerçek ve tüzel kişiler ile bu kişiler ile aynı risk grubunda olan diğer kişiler hakkında risk analizi ve değerlendirmesi ile takibinin yapılabilmesi için gerekli bilgi ve belgelerin temin edilmesi, temin edilen bilgi ve belgelerin teyit edilebilmesi için gerekli her türlü girişimde bulunulması, bu süreç için gerekli sistemsel düzenlemelerin yapılması ve işletilmesi için de kişisel verilerin işlenmesi Kanun kapsamında ilgili kişinin açık rızası alınmaksızın gerçekleştirilebilecektir.

2.1.2.3. Diğer Kanuni Yükümlülükler Gereği Veri İşleme ve Paylaşım

Kanun'un 5nci maddesinin ikinci fıkrasının (ç) bendi uyarınca bir hukuki yükümlülüğün yerine getirilebilmesi için veri işlenmesinin zorunlu olduğu hallerde veri sorumlusu, ilgili kişinin açık rızası olmasa dahi ilgili kişinin kişisel verilerini işleyebilecektir. Bankaların da bu doğrultuda tabi oldukları Bankacılık Kanunu, Sermaye Piyasası Kanunu gibi hem özel düzenlemelere hem de Anonim Şirket vasfında bulunmaları nedeniyle Türk Ticaret Kanunu, İş Kanunu gibi genel düzenlemelerde yer verilen hükümlere uyum sağlayabilmeleri için gerek müşterilerinin gerekse de çalışanlarının kişisel verilerini işlemeleri zorunludur.

Bu kapsamda bankaların hukuki yükümlülüklerini yerine getirebilmek için ilgili kişiden açık rıza alınmasına gerek olmayan haller kapsamında değerlendirilmek suretiyle yaptıkları başlıca işlemeler yalnızca bunlarla sınırlı olmamak üzere aşağıda sayılmaktadır:

- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun kapsamında kimlik tespiti ve teyidinin yapılabilmesi için kimlik bilgi

[23] "İlgili kişiye ait verilerin veri sorumlusu bir banka tarafından rızası olmaksızın babası ile paylaşılması karşısında kişinin Bankadan tazminat talep etmesi hakkında" Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/43 Sayılı Karar Özeti, www.kvkk.gov.tr

ve belgelerinin işlenmesi ve MASAK, Gelir İdaresi Başkanlığı ve adli kurumlar ile paylaşılması

- 5941 sayılı Çek Kanunu kapsamında çek hesabı sahiplerinin kişisel bilgilerinin işlenmesi ve Gelir İdaresi Başkanlığı ve Risk Merkezi ile paylaşılması
- 5411 sayılı Bankacılık Kanunu, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamında mevduat sahipleri, kredi borçluları, kart sahipleri ve ödeme hizmeti kullanıcılarının kişisel bilgilerinin işlenmesi ve Risk Merkezi, Tasarruf Mevduatı Sigorta Fonu ve Bankacılık Düzenleme ve Denetleme Kurulu ile paylaşılması
- 6362 sayılı Sermaye Piyasası Kanunu kapsamında yatırım ürünü sahibi gerçek kişilerin bilgilerinin işlenmesi ve Sermaye Piyasası Kurumu ve Yatırımcı Tazmin Merkezi ile paylaşılması
- 213 sayılı Vergi Usul Kanunu ve Türkiye'nin taraf olduğu uluslararası sözleşmeler kapsamındaki yükümlülüklere uyum sağlanabilmesi için gerçek kişi müşterilerin FATCA/CRS bildirim yükümlülüklerine ilişkin olarak bilgilerinin işlenmesi, BSMV, KKDF, Muhtasar Vergisi, Damga Vergisi, KDV, Kurumlar ve Geçici Vergisi, Form BA/BS vergilerinin ödenmesi ve raporlamaları için Maliye Bakanlığı ile kişisel verilerin paylaşılması
- Türk Borçlar Kanunu ve Türk Medeni Kanunu kapsamında gerçekleştirilen ipotek ve kefalet işlemlerinde ipotek veren/kefil olan gerçek kişilerin eşlerinin bilgilerinin işlenmesi
- 5411 sayılı Bankacılık Kanunu ve 6362 sayılı Sermaye Piyasası Kanunu kapsamında hesap ekstresi ve yatırım ekstresi hazırlanarak müşteriye gönderilebilmesi ve sesli görüşmelerin kaydedilmesi için kişisel veri işlenmesi
- 4857 sayılı İş Kanunu kapsamında işyeri sicil dosyasının oluşturulması ve iş ve sosyal güvenlik mevzuatı çerçevesinde oluşturulması gereken evrakların hazırlanabilmesi için gerçek kişi çalışan bilgisinin işlenmesi ve bunların Çalışma ve Sosyal Güvenlik Kurumu ile paylaşılması

2.1.3. İyi Uygulamalar

Bankaların kanunlarla izin verilen ya da hukuki yükümlülükleri çerçevesinde açık rıza olmaksızın gerçekleştirdiği bilgi/belge aktarımları kapsamında, gerçek kişi verisi içerir müşteri ve banka sırlarını kanunen açıkça yetkili kılınan mercilere açıklama yükümlülükleri, yetkili kılınan merciinin talep ettiği bilgi ile sınırlı olmalı ve Banka yetkili merciinin talebinde açıkça belirtilenden fazla bir gerçek kişi verisini kendi takdiri ile paylaşmamalıdır.

Örneğin, Kişisel Verileri Koruma Kurulu'nun vermiş olduğu bir kararda[24], mahkemece veri sorumlusundan ilgili kişi hakkında bazı kişisel verilerin talep edilmesi halinde, veri sorumlusunun gereğinden fazla kişisel veri aktarımında bulunmasının; Kanun'un 8'inci maddesinin (2) numaralı fıkrasında atıfta bulunulan Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer verilen hukuki yükümlülüğün yerine getirilmesi için zorunlu olması kapsamında değerlendirilmemiş ve Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiğine karar verilmiştir.

Dolayısıyla, bankalardan bilgi ve belge talep etmeye yetkili kurum ve kuruluşlarla yapılacak kişisel veri paylaşımlarında, paylaşılan bilgi/ belgenin talep edilen veriler ile sınırlı tutulması, bunun mümkün olmaması durumunda ilgili belgede yer alan diğer kişisel verilerin silinmesi/ maskelenmesi/ anonim hale getirilmesi suretiyle paylaşılması iyi uygulama örneği olarak değerlendirilebilir.

3- Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesi

Bir sözleşmenin kurulması ve ifası kapsamındaki yükümlülüklerin yerine getirilmesi için gerekli olan kişisel verilerin işlenmesi, ilgili kişinin açık rızasına tabi tutulmamıştır.

[24] Kişisel Verileri Koruma Kurulu'nun İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık) konulu kararı, www.kvkk.gov.tr

Örneğin, bankaların müşterileri olan veya olmayan ilgili kişilere yönelik sunduğu bazı hizmetler için (SMS ile kredi talebi gibi) talebin alınması, değerlendirilmesi ve cevaplanması süreçlerinde kişisel veri işlenmekte ancak taraflar arasında henüz bir sözleşme bulunmamaktadır. Banka ile ilgili kişiler arasındaki sözleşme ilişkisinin kurulma aşamasına (icaba davet ve icap) ilişkin veri işleme faaliyetleri açısından ilgili kişilerden açık rıza alınması gerekmemektedir.

Bir kredi sözleşmesindeki borç veren taraf olan bankanın, bildirimlerin yapılması için kişiye ait her türlü iletişim bilgisine sahip olması gerekmekte olup, bunun için kişinin açık rızasının alınmasına gerek bulunmamaktadır.

4- Meşru Menfaat[25]

Kişisel Verilerin Korunması Kanununun ("Kanun") 5'inci maddesinin 2'nci fıkrasının (f) bendi, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için zorunlu olması durumunda ilgili kişinin açık rızası alınmaksızın kişisel verilerin işlenebileceğini düzenlenmiştir.

<u>Meşru menfaatin tespiti nasıl yapılır?</u>

Veri sorumlusunun meşru menfaati hukuka aykırı olmayan menfaatini ifade etmektedir. Dolayısıyla bankanın hukuk düzeni içerisinde cevaz verilen hukuki veya iktisadi menfaatlerinin ancak belli koşullarda meşru menfaat kapsamında değerlendirilmesi mümkündür.

Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına

[25] Söz konusu kişisel veri işleme şartına ilişkin örneklere başlık altında yer verilmiş olmakla birlikte özellikle bu bölüm altında yer alan 4.2. ve 4.3. alt başlıklarının somut olay özelinde değerlendirilmesi gerekmektedir. Bu kapsamda verilen örnekler yerine göre açık rıza veri işleme şartı başta olmak üzere farklı veri işleme şartlarından birine de dayanabilecektir. Bu çerçevede meşru menfaat veri işleme şartının ancak veri sorumlularınca Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti'nde yer alan denge testinin yapılması sonucunda kabul edilebileceği göz önünde tutulmalıdır.

yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması önem arz etmektedir.[26]

Örneğin, çalışan bağlılığını artıran ödül ve primler uygulanması amacıyla veri işlenmesi durumunda meşru menfaate dayanılabilecektir.

<u>Kişisel verileri meşru menfaate dayalı kullanabilmek için inceleme nasıl yapılmalıdır?</u>

Meşru menfaatin tespitinde Kişisel Verileri Koruma Kurumu ("Kurum") tarafından yayımlanan "Veri sorumlusunun kanuni yükümlülüğü ve meşru menfaati çerçevesinde kişisel veri işlemesine ilişkin" 25/03/2019 tarihli ve 2019/78 sayılı karar meşru menfaate dayalı olarak kişisel veri işlenecek olması halinde, değerlendirmenin nasıl yapılması gerektiği konusunda yol gösterici nitelikte bir karardır.

Anayasa Mahkemesi, 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararı ile 12.01.2021 tarihli kararında[27] meşru menfaatin tespiti için denge testi işletmiş, böylelikle meşru menfaatin tespiti için ele alınması gereken ölçütleri de "ölçülülük" ilkesi çerçevesinde belirlemiştir.

Bu çerçevede banka, veri sorumlusu olarak meşru menfaate dayanmadan önce aşağıda yer alan her bir başlık özelinde değerlendirme yapmalıdır:

i. Amaç; Öncelikle ulaşılmak istenen amaç ve amacın gerçekleştirilmesinde meşru bir menfaatinin yararının olduğunu

[26] "Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru" hakkında Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, www.kvkk.gov.tr

[27] RG. 05.02.2021, s, 31386 (Çevrimiçi) https://www.anayasa.gov.tr/media/7232/2018-31036.pdf "•Başvuru konusu olayda çalışanın kurumsal e-postalarının denetlenmesi meşru menfaat kapsamında değerlendirilmiş, denetleme yapabilmek için kişisel verileri koruma mevzuatının da gerektirdiği üzere meşru menfaat bulunan işleme faaliyetinde açık rıza aranmamıştır"

ortaya koymalıdır. Meşru menfaat, halihazırda mevcut, belirli ve açık olmalıdır.

ii. Orantılılık; Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili amacın gerçekleştirilebilmesinde **ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi** gereklidir.

İlgili kişinin temel hak ve özgürlüklerine zarar vermediğinin tespit edilebilmesi için, veri sorumlusu ile ilgili kişi arasında "meşru menfaat testi" denilen üç aşamalı (amaç, gereklilik, orantılılık) bir ***denge testi*** yapılması, bu testin gerçekleştirilmesinde menfaatlerin tartılması gereklidir.[28]

Veri sorumlusu tarafından bu şartın varlığının test edilebilmesi için veri sorumlusu ile ilgili kişi arasındaki ilişki çerçevesinde ilgili kişinin makul beklentileri esas alınmalıdır. Bir başka ifadeyle, veri sorumlusu ve ilgili kişi arasındaki ilişkinin doğası gereği, ilgili kişi tarafından beklenebilecek işlemeler yönünden veri sorumlusunun meşru menfaatine dayanabilecektir.

iii. Gereklilik; **bu amacın gerçekleştirilebilmesi için kişisel veri işlenmesinin zorunlu/gerekli olması şarttır.** Buradaki zorunluluk, veri sorumlusunun kişinin verisini işlemek zorunda olmasıdır. Kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması gerekir.

Gereklilik ilkesi, kişisel verinin işlenmesi açısından, ulaşılmak istenen amacı gerçekleştirme bakımından aynı veya yakın derecede elverişli iki araçtan, daha az sınırlayıcı, yani daha yumuşak olan aracın seçilmesi gereğini ifade eder.[29] Bu noktada kişisel veri işlenmesi

[28] "Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru" ya ilişkin Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, www.kvkk.gov.tr

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

gerekli değil ise, bir başka ifadeyle "gereklilik testi" geçilemiyor ise anonim veri üzerinde çalışılması tercih edilmelidir.

Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulmalıdır.
Bununla birlikte;

- Kişisel verilerin bir veri kayıt sisteminde, amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,
- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması gereklidir.

Kişisel verilerin korunması hukukunda, somut olayın koşulları, yapılacak değerlendirmede büyük önem arz etmektedir. Bu sebeple, yapılan açıklamaların doğrultusunda gerçekleştirilecek meşru menfaat değerlendirmesi ve uygulamalara ait sorumluluk veri sorumlularına aittir. Aşağıda yer alan örneklere yalnızca konunun anlaşılmasını kolaylaştırma amacıyla belirli hizmet başlıkları altında yer verilmiştir.

Bu itibarla bankalar, meşru menfaat için gerekli değerlendirmeyi yaptıktan sonra ancak erişilebilir ve görünür bir şekilde aydınlatma yükümlülüğünü yerine getirmek ve başka bir amaçla kullanmamak kaydıyla ilgili kişilerin (kişisel verisi işlenen gerçek kişilerin) açık rızasını almaksızın verilerini kullanılabilecekleridir.

4.1. Bilgi Güvenliğinin Sağlanması Amacıyla

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ile bankalar için açıkça öngörülen yükümlülükler bulunmakla birlikte, bankalar, karşı karşıya kalabilecekleri güvenlik risklerini bertaraf etmek için gerekli güvenlik önlemlerini çeşitlendirmektedir.

4.1.1. Dolandırıcılık Tedbirleri

Bankalarca ilgili kişilerin işlem güvenliğinin sağlanması ve bankacılık işlem ve hareketlerindeki olağan dışı durumlar tespit edilerek gerekli tedbirlerin alınabilmesi amacıyla yapılan çalışmalar ilgili kişinin menfaatlerinin korunması çerçevesinde gerçekleştirilmektedir.

Örneğin; Müşterilerin olağan dışı davranışlarının tespit edilmesi ve anomali analizi yapılması için;

- Müşterinin daha önce alışveriş yaptığı lokasyonlar (şehir/ülke)
- Kullandığı cihazlara ait bilgiler (IP, IMEI telefon modeli, açar tercihi, işletim sistemi, zararlı yazılım tespiti için kullandığı uygulamalar vb.)
- Yapmış olduğu para transferlerine ilişkin bilgiler (alıcı TCKN/YKN/VKN, hesap/IBAN vb.) işlenebilmektedir.

4.2. Bankacılık Alanında Müşteri Gruplarının (Segmentasyon) Belirlenmesi Amacıyla

Bankalar nezdinde müşterilerin gruplandırılması temel olarak; müşterinin tâbi olduğu hizmet seviyesini belirlemeye, müşterinin bankalar ile olan ilişkisini ve ürün, kanal kullanımını anlamaya yönelik olarak müşteri verilerinin değerlendirilmesi sürecidir.

Müşterilerin gruplandırılması bu bağlamda, bankaların farklı birimlerine (Genel Müdürlük, Bölge ve Şube) ilişkin süreçlerin, rollerin, hedeflerin, çalışan sayılarının ve dolayısıyla bütçelerin ve maliyetlerin belirlenmesinde belirleyici unsurlar olmaktadır. Gruplandırma, bankaların faaliyetlerini sürdürebilmeleri için gerekli organizasyonel ve mali değerlendirmeyi yapmalarını, gelecek dönemler için öngörülerini oluşturmalarını sağlamaktadır. Bu durum, ilgili kişi ilişkilerinin yönetiminin yanı sıra, ilgili kişilerle uzun süreli ilişkiler kurulmasına ve müşterilere ihtiyaçlarına uygun hizmet verilmesine yardımcı olan bir eylemdir.

Tipik olarak, burada işlenen kişisel veriler, ilgili kişinin gelir ve gider gibi bilgilerinden oluşmaktadır. Bu bilgilerin işlenmesi ile ilgili müşteri

gruplarına doğru ürün/hizmet sunulması, bankaların tabi olduğu yasal düzenlemeler doğrultusunda, finansal tüketicinin korunması adına önem arz etmektedir.

Örneğin;

- Finansal gelir ve giderleri benzer olan kişilerden oluşturulan gruplara özel indirim, teklif veya ürün sunulabilmekte, her bir grup için özel pazarlama seçenekleri oluşturulabilmektedir.

Bu esaslar belirlenirken bankalarca aşağıdaki örneklere benzer hususlar dikkate alınabilir.

- İlgili kişilerin bankalardan aldıkları ürün ve hizmetlerin sunulması için gerekli olması nedeniyle elde edilmiş (sözleşmenin ifası için gerekli olan) veri kümesinin kullanılması
- Kullanılan verilerin veya segmentasyon analizi sonuçlarının gerekli teknik ve idari tedbirlerin alınması suretiyle korunması ve banka dışına çıkmasının engellemesi

Burada yapılan çalışmalarda, her bir olay bazında ölçülülük ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek esasları dikkate alınmalıdır.

4.3. Müşterilere Hitap Eden Ürün Hizmetlerin Tespiti Amacıyla

Çeşitli araştırmalar, veri temelli ekonomide tüketici beklentilerinin kendilerine özel ürün ve hizmetler sunulması olduğunu göstermektedir. Bu kapsamda, Bankanın finansal kaynaklarının verimli kullanımı ile müşteri ihtiyacının doğru şekilde karşılanması ve müşteri memnuniyetinin sağlanmasında müşteriye uygun ürün ve hizmetlerin sunulması önemlidir.

Bankalar bu ihtiyaca istinaden;

i. İlgili kişiler ile kurulan hizmet ilişkisi çerçevesi ile sınırlı olarak,
ii. İlgili kişinin makul beklentisi çerçevesinde kalarak,
iii. Somut olay özelinde ilgili kişinin de çıkarı olabileceğini gözetmek kaydıyla, sadece kullanılan ürün/hizmetle ile ilgili (doğrudan) pazarlama yapılması amacıyla, kişisel veri işleyebilmektedir.

Aşağıda bu gibi durumlara örnekler verilmektedir:

- Müşteriden sözleşme gereğince alınan meslek bilgilerinden yola çıkılarak, kamu çalışanlarına sunulacak bir kampanyanın sadece kamu çalışanlarına ulaşması sağlanabilmektedir.
- Belirli ürünlere yönelik (kredi, mevduat hesabı) uygulanan kampanyaların (indirim, avantaj, ilave taksit, puan vb.) sadece ilgili ürünü kullanan müşterilere iletilmesi sağlanabilmektedir.
- Müşteriler, banka ile kurduğu ilişki çerçevesinde, banka nezdinde bulunan ürün veya hizmetlerinin devamı niteliği taşıyan ürün/hizmetlerin sunulmasını ve yeni koşulların kendilerine bildirilmesini beklemektedir. Müşterinin yatırımın açıkta kalmaması için vadeli hesap sözleşmesinin vade sonunda müşteriye bildirilmesi ile muadil bir ürün teklif edilebilmektedir.
- Otomatik ödeme talimatı vermek isteyen ve kredili mevduat hesabı bulunmayan müşterilere, hesabında bakiye olmaması halinde ödemelerinde gecikmeye düşmemesi için kredili mevduat hesabı açılmasını isteyip istemediğinin sorulması

Bu aşamada kişisel veri işleme faaliyeti bakımından değerlendirmeler titizlikle yürütülmeli, kullanılacak olan kişisel veriler ölçülülük ilkesi çerçevesinde; özel nitelikli verilerden arındırılmış şekilde, müşterinin makul beklentisiyle uyumlu ve sınırlı olarak belirlenmelidir.

Bunun sağlanabilmesi için hukuka uygun olarak bankaca elde edilmiş verilerin aydınlatma metinlerinde belirtilmiş olması kaydıyla veri sorumlusu, ilgili kişiyi konu hakkında açık olarak bilgilendirmiş olmalıdır.

Tipik olarak, burada işlenen kişisel veriler;

- İlgili kişiler bankacılık ürün ve hizmetlerin sunulması veya kullanılması sırasında kurulan doğrudan temaslar kapsamında elde edilen,
- İçerisinde özel nitelikli kişisel veri bulundurmayan,
- Doğrudan müşterilerden edinilen kimlik, demografik ve iletişim bilgileri (örneğin, yaşı, eğitim durumu, nerede oturduğu) ile

- İlgili kişinin ürün/hizmet kullanım bilgilerinden (örneğin, işlem detaylarına girmeyecek veya hangi sektörlerde toplam ne kadar alışveriş yaptığı gibi toplulaştırılmış işlem verileri) oluşabilecektir.

Yukarıdaki örneklerde yer verildiği şekilde işlem yapılmaması müşterilere kendileri ile ilgili olmayan tekliflerin sunulması rahatsızlık verici düzeye ulaşabileceğinden aksi yönde uygulamalar ilgili kişilerin temel hak ve özgürlüklerinin ihlalini oluşturabilecektir.

Bu çerçevede yapılan kişisel veri işleme faaliyetlerinde ilgili kişinin aleyhine bir sonuç doğması halinde itiraz hakkını düzenlemiştir.[30] Bu hak, ilgili kişi meşru menfaat için veri sorumlusunun yaptığı denge testine müdahale edebileceği alandır. ilgili kişinin temel hak ve hürriyetlerine zarar vermemesi için veri sorumlusu profilleme neticesinde meşru menfaate dayalı olarak yaptığı bir faaliyet olması halinde, ilgili kişi ile iletişime geçtiği anda itiraz hakkını sunması önemlidir.

Örneğin ilgili kişiye reklam içerikli ileti gönderilmesi için "Ticari iletişim ve Ticari Elektronik iletiler Hakkında Yönetmelik" çerçevesinde kişinin onay vermiş olması kişinin makul beklentisinin tespitinde de önemli bir ölçüt olarak değerlendirilebilecektir.

4.4. Strateji Çalışmalarının Yürütülmesi

Müşterilerin iyi analiz edilmesi, pazar stratejileri belirlenmesinde önemli bir unsur olarak karşımıza çıkmaktadır. Bununla birlikte, ticari hayatta şirketlerin hizmet ve ürünlerini geliştirilebilmesi için müşterileri tanıma ve anlama ihtiyacı içindedirler.

Bu kapsamda banka nezdindeki müşteri verileri yapay zekânın devreye girmesi ile işlenmektedir. Bu aşamanın sonunda, kullanılan kişisel verilere geri dönülmesi mümkün olmayan, bir başka ifadeyle kişisel veri içermeyen,

[30] Kanunun 11. maddesi çerçevesinde ilgili kişi her zaman veri sorumlusuna başvurarak kendisi ile ilgili işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkına sahiptir.

genel davranışları gösteren bazı öngörülere ulaşılmaktadır.

Bankalarca bu öngörüler risk yönetimi, karlılık raporları, maliyetlerin azaltılması amacıyla kullanabildiği gibi bankanın kitlesel olarak tüm müşterileri için pazarlama stratejilerini belirleme gibi alanlarda etkin yaklaşımlar geliştirilmesinde kullanılabilmektedir.

Söz konusu analizler, müşteri bazında aksiyon alınma amacı güdülmeden gerçekleştirilmekte, banka faaliyetlerinin iyileştirilmesi, idari süreçlerin belirlenmesi ve yürütülmesi gibi amaçlara dayanmaktadır. Stratejik analiz sonuçlarına göre müşteri bazında aksiyon alınmasının söz konusu olması halinde, yeni amaç yönünden hukuki sebebin belirlenmesi zorunludur.

Örneğin; Bankalar hangi müşteri kitlesine hangi ürünlerin hitap edeceğini tespit etmek amacıyla, müşterilerin hangi ürünü aldığı, toplam maliyetleri, nerede alışveriş yapıldığı gibi davranış hareketlerini içeren veri tabanlarını inceleme ihtiyacında olabilmektedirler.
Bu kapsamda, hangi müşteri kitlesine ne tür ürün ve hizmetlerin sunulabileceğinin tahmin edilebilmesi ve etkin ürün kullanımı hedeflemesinde en sağlıklı sonuç veren yöntem olarak büyük veriye dayalı otomatik karar alma mekanizmaları tercih edilmektedir.
İlgili kişilerin ürün kullanma davranışlarının belirlenmesinde gerçek kişinin kimliğine ihtiyaç duyulamamakla birlikte kişisel veriler üzerinde çalışılması gerekebilmektedir.

Otomatik Karar Alma Mekanizmalarında Dikkat Edilmesi Gereken Ölçütler Nelerdir?

i. Hukuka uygun bir şekilde elde edilmiş kişisel verilerin, meşru amaçlar çerçevesinde, kullanılması öncesinde her somut olayın özellikleri göz önüne alınarak ayrıca değerlendirilmesi önem arz etmektedir. Bu noktada özellikle veri sorumlusu banka, daha hafif bir müdahale ile (anonim veri kullanarak vb.) istediği amaca ulaşabiliyorsa burada gerçekleştirilen faaliyetin meşru menfaate dayandığından bahsedilemeyecektir.

ii. İşlenecek kişisel verilerin türünü, niteliğini, kaynağını ve miktarını
iii. değerlendirmeli gereksiz ve aşırı işleme faaliyetlerinin önü alınmalıdır. Bu bağlamda mümkünse gerçek kişisel verileri modelleyen temsili veriler etkili bir çözüm olabilecektir. Veri işlemede risk (etki analizi) değerlendirmesi, yapay zekânın ve büyük verinin özellikleri gözetilerek, daha hassas bir şekilde yapılmalıdır.[31]
iv. Her durumda ilgili kişinin gizliliğinin korunmasının sağlanması için, müşterinin kimliğinin anonimleştirilmesi (anonymization) veya takma adlı hale getirilmesi (pseudonymization) suretiyle kişiye ait verilerin işlenmesi yolu tercih edilmelidir.
v. Anonimleştirme, kişisel verileri tanımlamanın muhtemel olmayan bir forma dönüştürme sürecidir. Yaşayan bir bireye bağlanamayan anonimleştirilmiş veriler, KVKK'ya tabi değildir. Dolayısıyla yapay zekânın oluşturduğu öngörü anonim bir veri olsa dahi oluşan bilgileri korunmasına devam edilmeli, kontrollü erişim ortamları veya sınırlayıcı lisansların kullanılması ve benzeri yöntemlerin uygulanması büyük titizlikle değerlendirilmelidir.
vi. Anonimleştirme sürecinde ilgili kişinin kimliğine ilişkin hiçbir bilgi tutulmazken, dolaylı tanımlayıcılar ve/veya bağlantılar yoluyla ilgili kişileri tanımlamak hala mümkün olabilmektedir. Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması, verilerin anonim olarak kullanılmasını sağlamak her zaman veri sorumlusunun yükümlülüğündedir.

Yapay zekânın çıktısı olan modellerin gerçek kişilere uygulandığı ikinci aşamaya geçildiğinde, amaca bağlı olarak yeniden bir hukuki sebep değerlendirmesi yapılması gerekmektedir. Bu aşama neticesinde oluşan bilginin ilgili kişi ile ilişkilendirilmek istenilmesi halinde, (örneğin oluşturulan profiller ve modellere göre kişiye özel ürün teklifleri yapılması durumunda) kişinin KVKK uyarınca uygun hukuka uygunluk sebebi bulunması zorunludur.

[31] Algoritmik Karar Verme ve Veri Koruması Yapay Zeka Çalışma Grubu, Şubat 2020, (çevrimiçi), https://www.istanbulbarosu.org.tr/files/docs/AlgoritmikKararVermeveVeriKorumas%C4%B1022020.pdf

4.5. Müşteri Memnuniyetinin Sağlanması

Gerek BDDK gerekse müşteriler tarafından bankaların tüketici şikâyetlerini ve müşteri ilişkilerini en iyi şekilde yönetmeleri beklenmektedir. Bu çalışmalar; veri işleme ile analiz faaliyetleri ve iletişimi kapsamaktadır. Bu kapsamda müşterinin ürün ve kanal kullanım detayları, şikâyet geçmişi gibi banka nezdinde tutulan veriler kullanılabilmektedir. Bu bilgilerin, bankaların sistemsel işleyişini devam ettirmek, müşteri aleyhine sonuç doğurabilecek hataları tespit etmek, düzeltmek ve bunlara karşı önlem almak amacıyla işlenmesi sonucunda müşteri deneyimi iyileştirilerek müşteri memnuniyeti de artırılmaktadır.

Örneğin; müşterinin mobil bankacılık kanalıyla alakalı bir şikayeti neticesinde müşterinin mobil bankacılıkta hangi menüleri kullandığı gibi verilerden yola çıkılarak müşteriye şikayet sebebiyle alakalı tatmin edici yanıtlarla dönülebilmesi ve genel kullanıcı deneyimi iyileştirilerek benzer şikayet sebeplerinin ortadan kaldırılması mümkün olmaktadır.

Büyük veri teknolojisi ile metinlerin analiz edilmesi, soru-yanıt makineleri, otomatik konuşma ve komut anlama, konuşma üretme, bilgi sağlama gibi başlıklardan faydalanabilmektedir.

Örneğin; bankalar çeşitli iletişim kanalları üzerinden topladıkları (ses, metin, görüntü, video, davranış, vb.) analiz edilebilir formata dönüştürülerek veriyi anlamaya çalışmakta böylelikle metinler içerisindeki referans kelimeler üzerinden ilgili kişinin talepleri anlaşılmakta ve otomatik olarak ilgili kişilerin talepleri karşılanmaktadır.

Bu analizlerin ilgili kişiler ile pazarlama yapılması ve ürün sunulması gibi amaçlar ile eşleştirilmesinin (profilleme yapılması) açık rıza gerektiren bir kişisel veri işleme faaliyetidir.

5- Bir Hakkın Tesisi ve Korunması İçin Zorunlu Olma

Bankaların faaliyetlerini güvenli bir şekilde yürütebilmesi maruz kaldıkları

risklerin belirlenmesine ve yönetilmesine bağlıdır.[32] Bankanın ticari menfaatini güvende tutmak amacıyla, alacakların tahsil edilmesi amacıyla kredi borçlusu müşteri ile iletişime geçmesi gerekebilmektedir.

Örneğin; Banka tarafından resmi bilgi paylaşım platformlarından (Risk Merkezi, vb.) veya BTK lisanslı kuruluşlar üzerinden yapılan ve TCKN bazlı sorgular ile rehberlik hizmeti veren kuruluşlardan temin edilen telefon numaraları bankaların alacaklarının tahsili için idari ve yasal takip aşamasında kullanılabilmektedir. Bu durum, ilgili kişiler açısından da kişinin gecikmeye düşen borçlarını ödeyerek takibe düşmemesine hizmet edecektir.

Banka, yaptığı sorgulamalar ile elde ettiği iletişim bilgilerini kullanarak ilgili kişilerle haberleşmesi sırasında gerekli kimlik doğrulama mekanizmalarını işletmeli, müşteriye ait bilgilerin üçüncü kişilerce ele geçirilmesini önlemelidir.

6- Bankalarca İşlenen Özel Nitelikli Kişisel Veriler
6.1. Özel Nitelikli Kişisel Veriler – Genel Olarak
6.1.1. Mevzuat

Özel nitelikli kişisel veriler, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") 6'ncı maddesinde sınırlı olarak sayılmıştır. Kanun'un ilgili maddesine göre özel nitelikli kişisel veriler, 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,

[32] Yaşar Alıcı, **Bankacılık Kanunu Şerhi,** Cilt II, On iki Levha Yayıncılık, İstanbul 2017, s. 893.

- ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri,
- biyometrik ve genetik verileridir.

Dolayısıyla, özel nitelikli kişisel verilerin kıyas yoluyla genişletilmesi mümkün değildir.

Kanun, söz konusu verilere özel bir önem atfetmekte ve bu verilerle ilgili daha sıkı bir düzenleme getirmektedir. Zira, bu veriler başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları dikkate alınmakta ve bu tür veriler özel nitelikli veri olarak kabul edilmektedir.

Bu doğrultuda Kanun uyarınca Kişisel Verileri Koruma Kurulunun ("Kurul") 31 Ocak 2018 Tarihli ve 2018/10 Sayılı Kararı[33] ile belirlenen yeterli önlemler alınmaksızın özel nitelikli verilerin işlenememesi öngörülmekte, ayrıca Kanun'un 6'ncı maddesinin ikinci fıkrasında özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu hükme bağlanmış olup 6'ncı maddenin üçüncü fıkrasında ise tahdidi olarak sayılan şartların varlığı halinde, yeterli önlem alınması şartı baki kalmak kaydıyla ilgili kişinin açık rızası aranmaksızın özel nitelikli kişisel verilerin işlenmesine imkân tanınmaktadır.

Buna göre;

a) İlgili kişinin açık rızasının olması,
b) Kanunlarda açıkça öngörülmesi,
c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

[33] "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31 Ocak 2018 tarihli ve 2018/10 sayılı Kararı, www.kvkk.gov.tr

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,
f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,
g) Siyasi, felsefî, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde işlenmeleri mümkündür.

Her halükarda ilgili kişiler, Kanun'un 10'uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de[34] düzenlenen hükümlere uygun şekilde bankalar tarafından kişisel verilerinin işlenmesi hakkında aydınlatılmalıdır.[35]

Öte yandan, Kanun'un 4'üncü maddesi, veri sorumlularının tüm kişisel veri işleme faaliyetlerinde uyum sağlamakla yükümlü olduğu genel ilkeleri ortaya koymaktadır. Özel nitelikli kişisel verilerin hassasiyeti göz önünde bulundurulduğunda; genel ilkelere uyum, söz konusu verilerin işlenmesinde ayrıca önem arz etmektedir. Bu kapsamda, özel nitelikli

[34] 30356 sayılı Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ, 2018

[35] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesi uyarınca ilgili kişinin açık rızasına veya Kanun'daki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmesi ve kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir. Bu bakımdan, işbu çalışmada yer alan özel nitelikli kişisel verilerin işlenmesi bakımından önerilen iyi uygulama örnekleri kapsamında aydınlatma yükümlülüğünün yerine getirilmesine ayrıca yer verilmeyecektir.

kişisel veri işlenmesini gerektiren her türlü veri işleme faaliyetinde "kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerinin gözetilmesi esastır. Nitekim, özel nitelikli verilerin işlenmesi kapsamında "ölçülülük" kavramı, Kurul'un 2019/81[[36]ve 2019/165[37] sayılı Kararlarında detaylı bir şekilde ele alınmıştır. Bu kapsamda, ölçülülük ilkesi uyarınca veri sorumlularının, ilgili kişilerden süreç özelinde hedeflenen meşru amaçlara ulaşmak için minimum düzeyde veri talep etmesi ve gerekli olmayan veri işlemeden kaçınması gerekmektedir. Bununla birlikte, kişisel verilerin işlenmesi, Kanunun 6'ncı maddesinde yer alan işleme şartlarından biri olsa dahi ölçüsüz nitelikte bir kişisel veri işleme faaliyetini meşrulaştırmamaktadır. Bu doğrultuda, özel nitelikli kişisel verilerin işlenmesi sırasında genel ilkelere uyuma azami hassasiyet gösterilmesi gerekmektedir. Örneğin bir iş yerinde insan kaynakları birimince çalışanların mali haklarının belirlenebilmesi için sendika üyeliği verisinin alınması ölçülü kabul edilecekken, aynı iş yerinin AR-GE birimince söz konusu verinin alınması ölçülü olarak kabul edilmeyecektir.[38]

6.1.2. Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Yeterli Önlemler

Kanun'un 6'ncı maddesinin dördüncü fıkrası uyarınca özel nitelikli kişisel verilerin işlenmesinde, Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. Bu kapsamda, özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler, Kurul'un 31 Ocak 2018 tarihli ve 2018/10 sayılı Kararı[39] ile belirlenmiştir. Buna göre, veri sorumluları tarafından:

[36] Kişisel Verileri Koruma Kurulu'nun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar Özeti, www.kvkk.gov.tr

[37] Kişisel Verileri Koruma Kurulu'nun 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, www.kvkk.gov.tr

[38] Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular Dökümanı- Kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi ne anlama gelir sorusuna verilen cevap.

[39] "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31 Ocak 2018 tarihli ve 2018/10 sayılı Kararı

(1) Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedür belirlenmelidir.
(2) Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmeli,
b) gizlilik sözleşmeleri yapılmalı,
c) verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve süreleri net olarak tanımlanmalı,
ç) periyodik olarak yetki kontrolleri gerçekleştirilmeli,
d) görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılmalı ve bu kapsamda kendisine tahsis edilen envanter iade alınmalıdır.

(3) Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise:

a) veriler kriptografik yöntemler kullanılarak muhafaza edilmeli,
b) kriptografik anahtarlar güvenli ve farklı ortamlarda tutulmalı,
c) veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanmalı,
ç) verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilmeli, gerekli güvenlik testleri düzenli olarak yapılmalı/yaptırılmalı, test sonuçları kayıt altına alınmalı,
d) verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmeleri yapılmalı, bu yazılımların güvenlik testleri düzenli olarak yapılmalı/yaptırılmalı, test sonuçları kayıt altına alınmalı,
e) verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanmalıdır.

(4) Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise:

a) özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunmalı,
b) bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışları engellenmelidir.

(5) Özel nitelikli kişisel veriler aktarılacak ise:

a) verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak veriler aktarılmalı,
b) verilerin taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle veriler şifrelenmeli ve kriptografik anahtar farklı ortamda tutulmalı,
c) farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmeli,
ç) verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmalı ve evrakı "gizlilik dereceli belgeler" formatında gönderilmelidir.

(1) Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumu'nun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberi'nde[40] belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.

Ayrıca Kurum tarafından yayınlanan Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber'de özel nitelikli verilerden biyometrik verilerin işlenmesinde aşağıda yer alan ilkelere dikkat edilmesi gerektiği belirtilmiştir:

- Temel hak ve özgürlüklerin özüne dokunmaması
- Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından

[40] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)

elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması

- Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması
- Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması
- Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin gecikmeksizin/derhal imha edilmesi
- İşleme amacı doğrultusunda sınırlı olmak üzere; veri sorumlularının Kanun'un 10'uncu maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi
- Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının Kanun'a uygun şekilde alınmış olması

6.2. Bankacılık Sektöründe Özel Nitelikli Kişisel Verilerin İşlenmesi

Bankacılık faaliyetleri kapsamında yoğun olarak işlenen özel nitelikli kişisel verilere ilişkin detaylı bilgiler aşağıda açıklanmaktadır.

6.2.1. Kimlik Belgesi Suretleri

Bankalar tarafından gerçekleştirilen işlemlerde kişilerden kimlik belgesi sureti alınması; Bankacılık mevzuatı gereği kimlik tespitinin zorunluluğu nedeni ile gerçekleştirilmekte olan faaliyetlerdendir.

5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un 27'nci maddesine dayanılarak oluşturulan 09 Ocak 2008 tarihli ve 26751 sayılı Resmi Gazete'de yayımlanan Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik'in ("Yönetmelik") 5'inci maddesi gereğince bankalar, (i) sürekli iş ilişkisi tesisinde tutar gözetmeksizin, (ii) işlem tutarı ya da birbiriyle bağlantılı birden fazla işlemin toplam tutarı seksen beş bin TL veya üzerinde olduğunda,

(iii) elektronik transferlerde işlem tutarı ya da birbiriyle bağlantılı birden fazla işlemin toplam tutarı yedi bin beş yüz TL veya üzerinde olduğunda, (v)

şüpheli işlem bildirimini gerektiren durumlarda tutar gözetmeksizin ve/veya (vi) daha önce elde edilen müşteri kimlik bilgilerinin yeterliliği ve doğruluğu konusunda şüphe olduğunda tutar gözetmeksizin kimliğe ilişkin bilgileri almak ve bu bilgilerin doğruluğunu teyit etmek suretiyle müşterilerinin ve müşterileri adına veya hesabına hareket edenlerin kimliğini tespit etmek zorundadır.

Yönetmelik'in 6'ncı maddesi gereğince ise gerçek kişilerin kimlik tespitinde, ilgilinin adı, soyadı, doğum yeri ve tarihi, uyruğu, kimlik belgesinin türü ve numarası, adresi ve imza örneği, iş ve mesleğine ilişkin bilgiler, varsa telefon numarası, faks numarası, elektronik posta adresi ile Türk vatandaşları için bu bilgilere ilave olarak anne, baba adı ve T.C. kimlik numarası alınır. İlgilinin adı, soyadı, doğum tarihi, T.C. kimlik numarası ve kimlik belgesinin türü ve numarasına ilişkin bilgilerin doğruluğu ise (a) Türk uyruklular için T.C. nüfus cüzdanı, T.C. sürücü belgesi veya pasaport ile üzerinde T.C. kimlik numarası bulunan ve özel kanunlarında resmi kimlik hükmünde olduğu açıkça belirtilen kimlik belgeleri ve (b) Türk uyruklu olmayanlar için pasaport, ikamet belgesi veya Bakanlıkça [Hazine ve Maliye Bakanlığı] uygun görülen kimlik belgesi üzerinden teyit edilir. Yetkililerce istenildiğinde sunulmak üzere teyide esas kimlik belgelerinin asıllarının veya noterce onaylanmış suretlerinin ibrazı sonrası okunabilir fotokopisi veya elektronik görüntüsü alınır yahut kimliğe ilişkin bilgiler kaydedilir.

Bu kapsamda, bankalarca kimlik teyidi amacıyla işlem gerçekleştiren kişilerden alınan kimlik belgesi suretleri, Kanun kapsamında özel nitelikli kişisel veriler olarak sayılan bir kısım verileri içerebilmektedir. Örneğin, nüfus cüzdanlarının eski versiyonlarında (pembe/mavi nüfus cüzdanlarında) arka yüzde 'din' ve 'kan grubu' haneleri bulunmaktadır. Bir başka kimlik tipi olan ehliyetlerde ise kan grubu bilgisi ve (eski tip ehliyetlerde) "kullandığı cihaz ve protezler" bilgisi yer almaktadır.

Bu verilerin, bankalarca kimlik tespitinin teyidi amacıyla ilgili kişinin din ve kan grubu gibi özel nitelikli kişisel verilerini de içeren arkalı önlü kimlik görüntüsünün talep edilmesi, Kanunun "Genel İlkeler" başlıklı 4 üncü

maddesinde düzenlenen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine uygun olmadığı gibi, Kanunun özel nitelikli kişisel verilerin işlenmesini düzenleyen 6 ncı maddesine de uygun olmayacağından söz konusu kişisel verileri içeren kısımların maskelenmesi uygun olacaktır.

Kimlik Belgesi Sureti Formatında Alınan Verilere İlişkin İyi Uygulama Önerileri:

Bankalar kimlik belgesi sureti alınan süreçlerini gözden geçirir ve ilgili mevzuata uyum kapsamında gerekli ise süreçlerini revize eder. Bu kapsamda:

- Kimlik belgesinde bulunan özel nitelikli verilerin Kanun'un 6'ncı maddesinde yer alan özel nitelikli kişisel veri işleme şartları bulunmaksızın işlenmemesi gerekir.
- Mümkün olması halinde kimlik belgesinde yer alan özel nitelikli verilerin işlenmeden sadece kimlik belgesinin ön yüzü/ilgili sayfası ile işlem yapılmalıdır.
- Bankanın ilgili süreçlerinde kimlik belgesi suretinde yer alan özel nitelikli kişisel veriler, kimlik tespiti harici bir amaçla işleniyor ise ve bu amaçla özel nitelikli kişisel veri işlenmesine ilişkin olarak Kanun'un 6'ncı maddesinde yer alan özel nitelikli kişisel veri işleme şartları bulunmuyor ise kimlik fotokopisindeki özel nitelikli veri hanelerinin karartılmasına ya da söz konusu verilerin kullanılmamasına yönelik teknik ve idari tedbirler alınmalıdır.

Bu başlık altında belirtilen hususlar, kimlik belgesi suretlerinin alındığı vekâletnameler ve imza sirkülerleri için de geçerlidir.

6.2.2. Sağlık Raporları

Sağlık verileri Kanunun 6 ncı maddesinin üçüncü fıkrası kapsamında yer alan öze nitelikli Kişisel verilerin işlenmesi şartlarına uygun olarak işlenebilecektir.

Örneğin:

5378 sayılı Engelliler Hakkında Kanun'un 7'nci maddesi ve "Bankacılık Hizmetlerinin Erişilebilirliğine Dair Yönetmelik"in 4'üncü maddesinin sekizinci ve dokuzuncu fıkraları uyarınca, %40 ve üzeri oranda engelli olduğuna ilişkin belgenin aslını veya banka tarafından onaylanacak suretini müşterisi olduğu bankaya ibraz eden ayırt etme gücüne sahip kişilerin engelli kabul edilerek, işbu Yönetmelikte tanınan haklardan yararlanacağı hüküm altına alınmıştır. Söz konusu düzenleme uyarınca, bankaların bu kapsamda belge ileten engelli müşterilerin engel durumuna ilişkin bilgi ve belgeleri tutma yükümlülüğü bulunmaktadır.

Bununla birlikte, 6698 sayılı Kanun'un 6'ncı maddesi uyarınca anılan Yönetmelik kapsamında engellik durumunun bankalarca kayıt altına alınması özel nitelikli kişisel verilerin işlenmesi olarak değerlendirilebilecek olup, bu kapsamda Kanun'un 6'ncı maddesinde öngörülen veri işleme şartlarının yerine getirilmesi gerekmektedir.

Sağlık Verilerinin İşlenmesine İlişkin İyi Uygulama Önerisi:

Bankalar müşterilerine ilişkin sağlık verilerinin işlendiği süreçlerini gözden geçirir ve ilgili mevzuata uyum kapsamında gerekli ise süreçlerini revize eder. Bu kapsamda:

- Mevcut durumda sağlık verilerinin işlendiği süreçlerde işleme şartlarına uyulup uyulmadığının kontrolünü sağlamalıdır.
- Sağlık verilerinin ilgili süreç özelinde gerçekleştirilmesi hedeflenen amaçlar kapsamında işlenmesine yönelik işleme şartları bulunmamakta ise sağlık verileri işlenmemelidir.
- Açık rıza gerektiren veri işleme faaliyetlerine yönelik olarak ise açık rıza beyanının açık rıza unsurlarına uygun şekilde alınıp alınmadığının kontrolü sağlanmalıdır.

6.2.3. Adli Sicil Kayıtları ve Ceza Mahkumiyeti ve Güvenlik Tedbirleriyle İlgili Mahkeme Kararları

Ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili kişisel verilerin Kanun 6'ncı

maddesinin üçüncü fıkrasında yer alan veri işleme şartlarının bulunması halinde işlenmesi mümkündür

Bankaların uygulamalarında mahkeme kararlarında yer alan bilgiler özellikle iki durumda işlenebilmektedir:

- Müşterilerin (örneğin çek yasaklılığı) bilgileri risk değerlendirmesi süreçlerinde kullanılmaktadır,
- Çalışan adaylarından ise işe girişlerde, işe alım sürecinin bir parçası olarak adli sicil kayıtları istenmektedir.

5941 sayılı Çek Kanunu'nun 2. maddesine göre *"Bankalar, çek hesabı açılması ile ilgili olarak bu Kanunla kendilerine verilen görev ve yükümlülükleri yerine getirirken, çek hesabı açtırmak isteyenin yasaklı olup olmadığını bu Kanun hükümlerine göre araştırırlar" ve "Bankalar, çek hesabı açtırmak isteyenlerin yasaklılık durumuna ilişkin Risk Merkezi ile adli sicil kayıtlarını ... hesabın kapatıldığı tarihten itibaren on yıl süreyle saklamakla yükümlüdür."* Buna göre, bankanın çek hesabı açmak isteyen müşterilerinin adli sicil kaydını işlemesi ve bu kaydın 10 yıl boyunca saklanması Kanun'un 6'ncı maddesinin üçüncü fıkrası uyrınca kanunlarda açıkça öngörülmesi hukuki sebebine dayalı olarak gerçekleştirilebilecektir.

Bankalar mahkeme kararlarında yer alan ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili kişisel verilerin işlendiği süreçlerini gözden geçirir ve ilgili mevzuata uyum kapsamında gerekli ise süreçlerini revize eder. Bu kapsamda bankalarca;

- Çalışan adaylarının ceza mahkûmiyet (adli sicil) bilgilerinin istenmesi kanunlarda açıkça öngörülen bir süreç olmadığından bu bilgilerin toplanmaması tercih edilebilir.
- Çek yasaklılığı değerlendirmesi yapılabilmesi için müşterinin adli sicil kaydı, ayrıca bir açık rıza olmaksızın işlenebilecektir. Ancak adli sicil kaydının çek yasaklılığı değerlendirmesi dışında başkaca bir amaç için kullanılması durumunda, söz konusu amaç kapsamında adli sicil kaydı verilerin işlenmesi için ayrıca Kanun'un 6'ncı maddesinde belirtilen özel nitelikli kişisel veri işleme şartlarından en az birinin mevcut olması gereklidir.

6.2.4. Çalışanları Sağlık Verileri

Sağlık verileri Kanun'un 6'ncı maddesinin 3'üncü fıkrasında yer alan veri işleme şartları kapsamında işlenebilecektir.

Sağlık Verilerinin İşlenmesine İlişkin İyi Uygulama Önerileri:

Bankalar çalışanlarına ilişkin sağlık verilerinin işlendiği süreçlerini gözden geçirir ve ilgili mevzuata uyum kapsamında gerekli ise süreçlerini revize eder. Bu kapsamda bankalar:

- Çalışanlara ilişkin sağlık verileri amaçla bağlantılı, sınırlı ve ölçülü olmak kaydıyla işlenir ve iş yeri hekimi, bazı departmanların çalışanların sağlık verilerine erişmesi gerekiyor ise, bu sağlık bilgilerine ilişkin erişim yetkilendirmesi / kısıtlanması uygulanır ve banka içerisinde sadece belirli kişilerin / departmanların sağlık verilerine hukuki sebebi ortaya konulmak suretiyle erişebilmesi sağlanır.

1. "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı gereği sağlık verileri de dahil olmak üzere özel nitelikli veriler şifrelenmiş bir şekilde muhafaza edilmeli, veriler üzerindeki hareketler loglanmalı, erişim yetkilendirmesi yapılmalı ve Karar'da yer verilen diğer önlemler alınmalıdır.
2. Mevcut durumda, her halükarda, bankaların çalışanların sağlık verilerini işlemesi gerekmesi sebebiyle, bankalar çalışanın açık rızasını temin etmelidir.

6.2.5. Sigorta Acentesi Sıfatıyla Alınan Sağlık

Sigorta acenteleri bir sözleşme ile bağlı bulundukları sigorta şirketlerinin temsilcileridir. Sigorta faaliyetinde bulunacak olan bankalar, 5411 sayılı Bankacılık Kanunu'nun 3'üncü maddesinde tanımlanan mevduat bankalarıve

katılım bankaları ile kalkınma ve yatırım bankalarıdır. Sigorta Acenteleri Yönetmeliği 13'üncü maddesinde sigorta acenteliği yapacak bankaların ne tür hukuki ve usulü yükümlülüklerinin olduğu düzenlenmektedir.

Bankalar yukarı bahsi geçen mevzuat hükümleri uyarınca sigorta acenteliği sıfatıyla sağlık verileri işlemektedirler. Bu konu işlenmesi "Bankaların Acente Sıfatıyla Hareket Ettiği Durumlar" başlığı altında ayrıntılı olarak açıklanmıştır.

6.3. Kimlik Doğrulamada Kullanılan

Biyometrik verinin tanımı Kanun'da yer almamaktadır ancak Kişisel Verileri Koruma Kurumu ("Kurum") tarafından yayımlanmış olan "Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber"e ("Rehber") göre biyometrik veri kişinin fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özelliklerini veri işleme sonucunda ortaya çıkaran ve ortaya çıkarılan özellikler kişinin kimliğini tanımlamaya yarayan ya da kişinin kimliğini doğrulayan kişisel verilerdir.

Rehber'e göre biyometrik veriler fizyolojik ve davranışsal olarak iki türe ayrılmıştır. Fizyolojik biyometrik veriler kişinin parmak izi, retinası, avuç içi, yüzü, el şekli, irisi gibi fizyolojik nitelikteki biyometrik verilerdir. Bunun yanı sıra, kişinin yürüyüş biçimi, klavyeye basış biçimi, araba sürüş biçimi gibi veriler ise Rehber'de davranışsal biyometrik veriler olarak belirtilmiştir.

Biyometrik veriler Kanun'un 6'ncı maddesinin 3'üncü fıkrasında yer alan veri işleme şartları kapsamında işlenebilecektir. Ayrıca, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması gerekmektedir. Bu sebeple veriler işlenecekleri amacın gerçekleştirilmesi ile ölçülü olarak işlenmelidir. Bu kapsamda, kişisel verilerin toplanması ve işlenmesi sırasında, kişisel verilerin korunması hakkına en az zarar verecek, yani en uygun aracın seçilmesi ölçülülük ilkesinin gereğidir.

Burada belirtilmelidir ki 1 Nisan 2021 tarihli ve 31441 sayılı Resmî Gazete'de yayımlanan Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine Ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik'in

8 inci maddesi uyarınca "uzaktan kimlik tespiti sürecinde kişinin yüzü ile kimlik belgesi üzerinde yer alan fotoğrafın biyometrik karşılaştırması yapılır". Bahsi geçen bu yönetmelik uyarınca bankalara, uzaktan müşteri edinme süreçlerinde müşterilerin biyometrik verilerini işleme yükümlülüğü getirilmiştir. Yönetmeliğin 6 ncı maddesine göre "uzaktan kimlik tespiti sürecinde, kişinin uzaktan kimlik tespitinin yapılması amacıyla özel nitelikli kişisel verilerden sadece biyometrik verisi kullanılabilir ve kişinin buna dair açık rızası elektronik ortamda kayıt altına alınır". Yönetmeliğin ilgili maddesi sebebiyle uzaktan müşteri edinme süreçlerinde işlenen biyometrik veriler için Kanunun 6 ncı maddesi uyarınca ilgili kişilerden açık rıza alınması gerekecektir. Ancak burada belirtilmelidir ki, ilgili yönetmelik, bankaları, uzaktan müşteri edinme sürecinde kişilerin biyometrik verilerinin işlenmesi için açık rıza almakla yükümlü kılmaktadır. Rehbere göre biyometrik verilerin işlendiği durumlarda veri sorumluları, biyometrik verilerin bulut sistemlerinde yalnızca kriptografik yöntemler kullanılarak muhafaza edilmesi, biyometrik verilerin işlendiği yazılım üzerindeki kullanıcı işlemlerinin izlenebilir ve sınırlanabilir olması, biyometrik çözümü kullanamayan veya kullanmaya açık rızası olmayan ilgili kişiler için herhangi bir kısıtlama veya ek maliyet olmaksızın alternatif bir sistem sağlanması ve biyometrik veri işleme sürecinde yer alan personel biyometrik verilerin işlenmesi hususunda özel eğitimler alması gibi teknik ve idari tedbirleri almalıdır.

Burada belirtilmelidir ki, biyometrik veri işleme faaliyeti Kanun'un 4'üncü maddesindeki genel ilkelere aykırılık teşkil etmemelidir. Kurul'un 2019 yılında vermiş olduğu iki kararda[41], veri sorumlusu olan spor salonu şirketinin, spor salonuna giriş - çıkışlarda avuç içi okuma teknolojisinin kullanılması incelenmiştir. Buna göre Kurul, spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken gerçekleşen biyometrik veri işleme faaliyetini Kanun'un 4'üncü maddesinde belirtilen

[41] Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 Sayılı Karar Özeti

"kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine aykırı bulmuştur.

Bahsi geçen karar ışığında, biyometrik veri işlenen süreçlerde eğer biyometrik veri işlenmesi ile ulaşılmak istenen amaca biyometrik veri işlenmeden de ulaşılması mümkün ise (ör: giriş-çıkışlarda avuç içi yerine kimlik kartı kullanılması), biyometrik veri işlenmesini gerektirmeyen alternatif bir yolun tercih edilmesi uygun olacaktır.

Kimlik Doğrulamada Kullanılan Biyometrik Veriler ile İlgili Kişisel Verilerin İşlenmesine İlişkin İyi Uygulama Önerileri:

Bankalar kimlik doğrulamada kullanılan biyometrik veriler ile ilgili kişisel verilerin işlendiği süreçlerini gözden geçirir ve ilgili mevzuata uyum kapsamında gerekli ise süreçlerini revize eder. Bu kapsamda bankalar:

- Eğer mümkün ise biyometrik veriler işlememelidir (örneğin eğer kişisel verilerin korunması hakkına daha az zarar verecek başka bir araç mümkün ise biyometrik veriler toplanmamalıdır).
- Mevcut durumda biyometrik verilerinin işlendiği süreçlerde mutlaka Kanunun 6 ncı maddesi hükümlerine ve konuya ilişkin diğer mevzuata uyum sağlanmalıdır.
- Biyometrik verilerin işlendiği durumlarda, veri sorumlularınca Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber'de belirtilen teknik ve idari tedbirler alınmalıdır.

VIII. Kişisel Verilerin Aktarılması

Kişisel verilerin aktarılması, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") 3'üncü maddesinde işleme tanımı içerisinde yer bulmaktadır. Bununla birlikte, ayrıca Kanunun 8 inci ve 9 uncu maddelerinde özel olarak düzenlenerek iki başlık altında ele alınmıştır.

Belirtilen maddeler kapsamında hem kişisel hem de özel nitelikli kişisel veriler yer almaktadır. Kanun'un 8'inci maddesinde kişisel verilerin yurtiçinde aktarılmasına ilişkin hükümlere, 9 uncu maddesinde ise kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlere yer verilmiştir.

Kanun'da yer alan düzenlemelere istinaden, verilerin hukuka uygun bir şekilde aktarılabilmesi için belirtilen maddelerde yer alan şartların yerine getirilmiş olması gerekir.

1. Kişisel Verilerin Yurt İçinde Aktarılması

Kanun'un 8'inci maddesinde, kişisel verilerin yurt içinde aktarılmasına ilişkin usul ve esaslar düzenlenmektedir.

Kanun'un kendi sistematiği içerisinde belirlenen genel ilkeler çerçevesinde işlenmek üzere elde edilen kişisel verilerin, 8'inci madde hükmü uyarınca ilgili kişinin açık rızası alınmak suretiyle üçüncü kişilere aktarılabileceği hüküm altına almıştır. Ancak, açık rıza Kanundaki kişisel veri işleme şartlarından biridir ve diğer kişisel veri işleme şartlarına göre karşılaştırmalı bir üstünlüğü bulunmamaktadır. Açık rıza veri işleme faaliyetine hukukilik kazandıran yegâne unsur değildir.

Kanun, kişisel verilerin işlenmesi ile bu verilerin yurt içinde aktarılması bakımından da aynı şartları aramaktadır. Dolayısı ile kişisel veriler ilgili kişinin açık rızası aranmaksızın üçüncü kişilere aktarılabilecek, ancak aktarım için de Kanun'un 5'inci ve 6'ncı maddelerindeki şartların ayrıca aranması gerekecektir.

Buna göre, kişisel veriler;

i. Kanunlarda açıkça öngörülmesi,
ii. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
iii. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
iv. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
v. İlgili kişinin kendisi tarafından alenileştirilmiş olması,
vi. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
vii. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumlarında veri sorumlusu tarafından, ilgili kişinin açık rızası alınmaksızın yurt içindeki üçüncü kişilere aktarılabileceklerdir.

Kanunun 6 ncı maddesi uyarınca, 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,

a) İlgili kişinin açık rızasının olması,
b) Kanunlarda açıkça öngörülmesi,
c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,
d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik,

tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması,

hâlinde yurt içindeki üçüncü kişilere aktarılabilecektir.

Ayrıca özel nitelikli kişisel verilerin işlenmesine ilişkin yeterli önlemler ise 07.03.2018 tarihli ve 30353 sayılı Resmî Gazete'de yayımlanan 31.01.2018 tarihli ve 2018/10 sayılı Kurul Kararı[42] ile belirlenmiştir. Bununla birlikte, Kanun'un 8'inci maddesinin üçüncü fıkrasında kişisel verilerin yurt içinde aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlenmiştir.

Bu noktada ifade edilmesinde fayda görülmektedir ki, 5411 sayılı Bankacılık Kanununun "Sırların saklanması" başlıklı 73 üncü maddesinin üçüncü fıkrasında diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgilerin anılan maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 6698 sayılı Kanun uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamayacağı ve bunlara aktarılamayacağı hükme bağlanmıştır. Bununla birlikte, 04.06.2021 tarihli ve 31501 sayılı Resmî Gazetede yayımlanan Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik ile müşteri sırrı niteliğindeki bilgilerin paylaşım ve aktarımlarına ilişkin kapsam, şekil, usul ve esasları belirlenmiştir.

[42] "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10

Dolayısıyla, 6698 sayılı Kanunun gerek 4'üncü maddesinin 1'inci fıkrasında yer verilen *"Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir."* gerek 8'inci maddesinin 3'üncü fıkrasında öngörülen "Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükümleri uyarınca müşteri sırrı niteliğindeki kişisel verilerin aktarımı bakımından 5411 sayılı Kanunda öngörülen mezkûr düzenleme ile anılan Yönetmelik hükümlerinin göz önünde bulundurulması gerekmektedir.

Öte yandan belirtmek gerekir ki, veri sorumlusu sıfatına sahip bir tüzel kişiliğin bünyesinde gerçekleşen veri aktarımı, üçüncü kişiye yapılan aktarım olarak değerlendirilemeyecek; kişisel verilerin, bir tüzel kişiliğin bünyesinde faaliyet gösteren çalışanlar veya farklı birimler arasında el değiştirmesi, bu anlamda kişisel verilerin üçüncü kişilere aktarımı sayılamayacaktır.[43] Dolayısıyla, kişisel verilerin bir bankanın farklı iş birimleri arasında el değiştirmesi, kişisel verilerin aktarılması niteliğinde olmadığından, Kanun'un ilgili maddelerinde yer alan hükümlere tabi değildir. Ancak, Kişisel Verileri Koruma Kurulunun 04.07.2018 tarihli ve 30468 sayılı Resmi Gazete'de yayımlanan 31.05.2018 tarihli ve 2018/63 sayılı İlke Kararında *"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, (...)"*[44] karar verilmiştir. Dolayısıyla, Kanun'un 4'üncü maddesinin ikinci fıkrasında yer verilen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de riayet edilerek aynı veri sorumlusu bünyesinde

[43] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s.89

[44] Veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu verileri işlemesi hususunun değerlendirilmesine ilişkin 31.05.2018 tarihli ve 2018/63 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/5248/2018-63

bulunan farklı bölümler ya da kişiler arasında gerçekleştirilecek kişisel veri paylaşımlarının da sınırlı bir kapsamda gerçekleştirilmesi gerekmektedir. Bir tüzel kişi bünyesinde farklı birimler arasında veri paylaşımı yapılmasının aksine, aynı şirketler topluluğu bünyesinde yer alan farklı tüzel kişiler arasında veri aktarımı gerçekleştirilmesi, Kanun'un 8'inci maddesi kapsamında veri aktarımı sayılacaktır.

Nitekim, Kişisel Verileri Koruma Kurulunun bir kararında; *"Bir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirketler arasında veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı olarak değerlendirildiği,* bu itibarla aynı şirketler topluluğu bünyesinde yer alan veri sorumluları arasında gerçekleşecek veri aktarımında da 6698 sayılı Kişisel Verilerin Korunması Kanununun 8 inci maddesi hükümlerinin esas alınması gerektiği (...)" belirtilmiştir.[45] Bu doğrultuda, bankaların bünyelerinde yer aldıkları şirketler topluluğu içerisindeki diğer şirketlere yaptığı kişisel veri aktarımları "üçüncü kişiye veri aktarımı" kategorisinde yer aldıklarından, Kanun'un ilgili maddelerinde yer verilen hükümlere tabidir.

1.1. KVKK Madde 8/3 Uyarınca Yapılabilecek Kişisel Veri Aktarımları

Kanun'un 8'inci maddesinin üçüncü fıkrasında, kişisel verilerin üçüncü kişilere aktarılmasına ilişkin *diğer kanunlarda yer alan hükümlerin saklı olduğu* ifade edilmektedir. Kanun koyucu, kişisel verilerin aktarılmasına ilişkin ana kuralı Kanun'da belirlemekle birlikte, diğer kanunlarda konuya ilişkin olarak yer alan düzenlemelerin saklı olduğunu da düzenlemiştir.

Hâlihazırda kişisel verilerin korunmasına değinen ulusal düzeyde çok sayıda kanuni düzenleme mevcuttur. 5411 sayılı Bankacılık Kanunu da bu düzenlemelerden birisidir.

Bu itibarla, 6698 sayılı Kanunun 8 inci maddesinin üçüncü fıkrası uyarınca gerek 5411 sayılı Kanunda gerek diğer kanunlarda yer verilen düzenlemeler çerçevesinde kişisel veriler aktarılabilecektir.

[45] "İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması" https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi

1.1.1 Bankalardan Bilgi Talep Etmeye Yetkili Mercilere Gerçekleştirilen Kişisel Veri Aktarımları

Bankalar, Kanun uyarınca, bilgi aktardıkları kurum ve kuruluşların kendi kuruluş kanunları ve diğer kanunlardan kaynaklanan bilgi talep etme yetkilerine istinaden yetkili mercilere kanunlardaki sınırlamalar çerçevesinde, ilgili kişilerin açık rızasına gerek olmaksızın kişisel veri aktarımında bulunabilirler. Mahkemeler, savcılıklar, T.C. Bankacılık Düzenleme ve Denetleme Kurumu ("BDDK"), Sayıştay, Sermaye Piyasası Kurulu ("SPK"), Türkiye Cumhuriyet Merkez Bankası ("TCMB"), Tasarruf Mevduatı Sigorta Fonu ("TMSF"), Gelir İdaresi Başkanlığı ("GİB"), Sosyal Güvenlik Kurumu ("SGK"), Mali Suçları Araştırma Kurumu ("MASAK") ve bunlarla sınırlı olmamak üzere kanunlar kapsamında bankalardan bilgi ve belge talep etmeye yetkili mercilere kişisel veri aktarımı yapılabilecektir.

Bankaların, müşteri ve banka sırlarını kanunen açıkça yetkili kılınan mercilere açıklama yükümlülükleri, Bankacılık Kanunu'nun 73'üncü ve 159'uncu maddelerine göre mercilerin "ilgili konularda sordukları soruların cevaplandırılması" ile sınırlandırılmıştır. Aşağıda, istisna kapsamında değerlendirilen merciler ile bilgi paylaşımına ilişkin örneklere yer verilmektedir:

- **Savcılık ve mahkemelere verilen bilgi ve belgeler**

  5271 sayılı Ceza Muhakemesi Kanunu'nun "Bilgi isteme" başlıklı 332'nci maddesinde yer alan "Suçların soruşturma ve kovuşturması sırasında Cumhuriyet savcısı, hâkim veya mahkeme tarafından yazılı olarak istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Eğer bu süre içinde istenen bilgilerin verilmesi imkânsız ise, sebebi ve en geç hangi tarihte cevap verilebileceği aynı süre içinde bildirilir. Bilgi istenen yazıda yukarıdaki fıkra hükmü ile buna aykırı hareket etmenin Türk Ceza Kanununun 257'nci maddesine aykırılık oluşturabileceği yazılır. Bu durumda haklarında kamu davasının açılması, izin veya karar alınmasına bağlı bulunan kişiler hakkında, yasama dokunulmazlığı saklı kalmak üzere, doğrudan soruşturma

yapılır." hükümlerine istinaden Cumhuriyet savcısı, sulh ceza hâkimi veya mahkemeler tarafından istenen bilgilerin bankalarca verilmesi zorunlu olduğundan bu kapsamda kişisel veri aktarımı yapılabilecektir. 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 221'inci maddesinin ilk ve ikinci fıkralarına göre "Mahkeme, üçüncü kişi veya kurumun elinde bulunan bir belgenin taraflarca ileri sürülen hususun ispatı için zorunlu olduğuna karar verirse, bu belgenin ibrazını emreder. Belgeyi ibraz etmesine karar verilen herkes, elindeki belgeyi ibraz etmek; belgeyi ibraz edememesi hâlinde ise bunun sebebini delilleri ile birlikte açıklamak zorundadır. Mahkeme yapılan açıklamayı yeterli görmezse, bu kimseyi tanık olarak dinleyebilir." Hukuk mahkemeleri tarafından anılan hükme istinaden bankalara iletilen belge talepleri söz konusu olduğunda, söz konusu belgeler kapsamında yer alan kişisel veriler de mahkemeye aktarılabilecektir.

- **Kamuyu Aydınlatma Yükümlülüğü altında açıklama yapılması**

6362 sayılı Sermaye Piyasası Kanunu'nun ("6362 sayılı Kanun") 136'ncı maddesinin 5'inci fıkrasına göre, kendi sermaye piyasası araçlarını halka arz ederek veya halka arz etmeksizin satan bankalar ile 6362 sayılı Kanun'da tanımı yapılan yatırım hizmetleri ve faaliyetlerinde bulunan bankalar, bu faaliyetleri ile sınırlı olarak, 6362 sayılı Kanun hükümlerine tabidir. Yukarıda zikredilen hüküm çerçevesinde bankalar da Sermaye Piyasası Kurulu'nun, 6362 sayılı Kanun'un 15'inci maddesinin verdiği yetkiye istinaden yayımladığı II-15.1 sayılı "Özel Durumlar Tebliği" kapsamında bulunmaktadır. Dolayısıyla, bu kapsamda kişisel veriler açıklanmak suretiyle aktarım faaliyeti gerçekleştirilebilecektir.

- **Finansal Raporların yayımlanması ve yetkili mercilere aktarılması**

Bankacılık Kanunu'nun 39'uncu maddesinin 3'üncü fıkrasına ve buna istinaden yayımlanan Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Yönetmeliğinin 14'üncü maddesine göre bankaların finansal raporlarının BDDK'ya ve Türkiye Bankalar Birliğine ("TBB") ya da Türkiye Katılım Bankaları Birliğine sunulması,

Resmi Gazete'de ilan edilmesi ve banka ve kuruluş birlikleri tarafından internet sayfalarında yayımlanması gerekmektedir. Dolayısıyla söz konusu finansal raporların sunumu veya yayımlanması kapsamında kişisel veri aktarımı yapılabilecektir

- **İşçi, gemi adamı ve gazetecilerini tihkak ödemelerinin yapıldığı hesaplara ait bilgilerin kanunla yetkili kılınan mercilere aktarılması**

6098 sayılı Borçlar Kanunu, 5953 sayılı Basın Mesleğinde Çalışanlarla Çalıştıranlar Arasındaki Münasebetlerin Tanzimi Hakkında Kanun, 854 sayılı Deniz İş Kanunu ile 4857 sayılı İş Kanunu kapsamında çalıştırılan işçi, gemi adamı ve gazetecinin ücret, prim, ikramiye ve bu nitelikte her çeşit istihkak ödemelerinin özel olarak açılan banka hesabına yapılması halinde, bu hesaplara ilişkin bilgi ve belgelerin Çalışma ve Sosyal Güvenlik Bakanlığı, Hazine ve Maliye Bakanlığı ve bunlara bağlı ve ilgili kurum ve kuruluşlara verilmesi kapsamında kişisel veri aktarımı gerçekleştirilebilecektir

- **Gelir testi yapılmasına ve sosyal yardım hak sahiplerinin belirlenmesine ilişkin bilgilerin kanunla yetkili kılınan mercilere aktarılması**

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 8'inci ve 100'üncü maddelerinin uygulanması ile genel sağlık sigortalılığında gelir testinin yapılmasına ilişkin bilgi ve belgelerin Sosyal Güvenlik Kurumuna ve il veya ilçe sosyal yardımlaşma ve dayanışma vakıflarınca yapılan sosyal yardım hak sahiplerinin tespiti ile gelir testi işlemlerinin yürütülmesi amacıyla Aile ve Sosyal Hizmetler Bakanlığı Sosyal Yardımlar Genel Müdürlüğüne verilmesi kapsamında anılan kuruluşlara kişisel veri aktarımı yapılabilecektir.

- **Kısmen veya tamamen karşılığı bulunmayan çeki keşide edenlerin bankaca bilinen adreslerinin çek hamiline verilmesi**

5941 sayılı Çek Kanunu'nun 2'nci maddesinin ikinci fıkrasına göre, çekin karşılığının kısmen veya tamamen bulunmaması halinde, çek keşidecisinin bankaca bilinen adresleri, talebi halinde çek hamiline veya çek hamilinin yetkili vekiline verilecektir. Bu kapsamda anılan hüküm uyarınca kişisel veri aktarımı gerçekleştirilebilecektir. bilgiler arasında kişisel verilerin de yer alması halinde, anılan hüküm uyarınca aktarım yapılması mümkündür.

- **Sayıştaya Verilecek bilgiler**

6085 sayılı Sayıştay Kanunu'nun 6'ncı maddesinin ikinci fıkrasına göre Sayıştay, denetimine giren işlemlerle ilgili her türlü bilgi ve belgeyi bankalardan isteyebilmektedir. Sayıştay'a verilebilecek

- **İcra ve İflas Müdürlüklerine Verilecek bilgiler**

2004 sayılı İcra ve İflas Kanununun 367'nci maddesine göre gerçek ve tüzel kişiler icra veya iflas dairelerinin borçlunun mevcuduna dair isteyeceği bütün bilgileri vermek zorundadır.

1.1.2. Şüpheli İşlem Bildirim Zorunluluğu Çerçevesinde Gerçekleştirilen Kişisel Veri Aktarımları

5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un 4'üncü maddesi gereğince; yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması halinde, bu işlemlerin yükümlüler tarafından MASAK'a bildirilmesi zorunludur.

5549 sayılı Kanun'un 10'uncu maddesine göre; kanun gereğince yükümlülüklerini yerine getiren gerçek ve tüzel kişiler hiçbir şekilde hukukî ve cezaî bakımdan sorumlu tutulamaz.

Şüpheli işlem bildirimleri bankalar açısından kanunda açıkça öngörülen

bir yükümlülük olduğundan bu kapsamda kişisel veri aktarımı yapılması mümkündür.

1.1.3. Ana Ortak/Bağlı Ortaklıklara Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrasında; "Sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıkların konsolide finansal tablo hazırlama çalışmalarında, risk yönetimi ve iç denetim uygulamalarında kullanılmak üzere bilgi ve belge taleplerinin karşılanması sırasında banka ya da müşteri sırrı niteliğindeki bilgilerin öğrenilmesi sır saklama yükümlülüğü dışındadır." hükmü yer almaktadır.

Buna göre Türkiye'deki bir banka, hükümde yer alan şartları taşıyan ana ortaklığın bilgi ve belge taleplerini gizlilik sözleşmesi yapılması ve konsolide finansal tablo hazırlama çalışmaları, risk yönetimi iç denetim uygulamaları ile sınırlı kalınması şartıyla karşılayabilecektir. Söz konusu ana ortaklık, finansal kuruluş ya da başka bir teşebbüs olabilecektir.

1.1.4. Muhtemel Alıcılara Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrası kapsamında bankalar, doğrudan veya dolaylı pay sahipliği yoluyla sermayelerinin yüzde onunu ve daha fazlasını temsil eden paylarının satışı amacıyla muhtemel alıcıların yapacakları değerleme çalışmalarında kullanılmak kaydıyla, gizlilik sözleşmesi yapılması ve sözleşmede belirtilen koşullarla sınırlı kalınması şartıyla muhtemel alıcıların bilgi ve belge taleplerini karşılayabileceklerdir. Bu doğrultuda, bankaların kredileri de dahil varlıklarının ya da bunlara dayalı menkul kıymetlerinin satışı amacıyla yapılacak değerleme çalışmaları çerçevesinde, gizlilik sözleşmesi yapılması ve sözleşmede belirtilen koşullarla sınırlı kalınması şartıyla, muhtemel alıcıların bilgi ve belge talepleri karşılanabilecektir.

Bu kapsamda yapılan bilgi ve belge alışverişlerinde kişisel veri aktarımı

yapılması da mümkündür.

1.1.5. Bankalar ve Finansal Kuruluşlara Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrasına göre bankalar ve finansal kuruluşlar gizlilik sözleşmesi yapmak ve sözleşmede belirtilen amaçlarla sınırlı kalınmak kaydıyla kendi aralarında doğrudan doğruya her türlü bilgi ve belge alışverişinde bulunabilirler.

Bu kapsamda, bankalar ile diğer bankalar ve finansal kuruluşlar arasında her türlü bilgi alışverişi kapsamında kişisel veri aktarımı yapılması mümkündür.

1.1.6. Risk Merkezi, Bankalar Arası Kart Merkezi ve Kredi Kayıt Bürosu'na Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrası kapsamında gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla bankaların ve finansal kuruluşların, risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi bankaların sır saklama yükümlülüğü dışında tutulmuştur. Bankalarca Risk Merkezi, Bankalararası Kart Merkezi ("BKM") ve Kredi Kayıt Bürosu ("KKB")'na gizlilik sözleşmesi yapılmak ve belirtilen amaçlarla sınırlı olmak kaydıyla kişisel veri aktarımı yapılması mümkündür.

1.1.7. İştiraklere Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrası uyarınca, gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla bankaların ve finansal kuruluşların, risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi bankaların sır saklama yükümlülüğü dışında tutulmuştur. Bu kapsamda bankalar ile bankaların finansal kuruluşu niteliğindeki bağlı ortaklıkları arasındaki bilgi ve belge

paylaşımı kapsamında kişisel veri aktarımı yapılması mümkündür

1.1.8. Değerleme, Derecelendirme ve Destek Hizmeti Kuruluşlarına Gerçekleştirilen Kişisel Veri Aktarımları

Bankacılık Kanunu'nun 73'üncü maddesinin dördüncü fıkrası kapsamında bankalar ile değerleme, derecelendirme ve destek hizmetleri kuruluşları arasında gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla değerleme, derecelendirme veya destek hizmeti alınması ile bağımsız denetim faaliyetlerinde kullanılmak üzere bilgi ve belge taleplerinin karşılanması sırasında banka ya da müşteri sırrı niteliğindeki bilgilerin öğrenilmesi sır saklama yükümlülüğü dışında olup, bu kapsamda kişisel veri aktarımı yapılması mümkündür.

Bankaların destek hizmeti niteliği taşımayan hizmet alımlarına yönelik işlemlerde kullanılmak üzere bilgi ve belge paylaşımları gerekli tedbirlerin alınması, gizlilik sözleşmesi yapılması ve belirtilen amaçlarla sınırlı kalınması koşuluyla sır saklama yükümlülüğüne aykırılık teşkil etmediğinden, bu koşulların sağlanması halinde kişisel veri aktarımları yapılabilir.

1.2. İş Ortaklarına Gerçekleştirilen Kişisel Veri Aktarımları

Bankalar, müşterilerine sağladıkları bankacılık ürünleriyle bağlantılı olarak bir takım ek hizmet ve avantajları içeren kampanyalar düzenleyebilmekte, söz konusu kampanyalar kapsamında üçüncü taraf kişi ve kuruluşlarla iş ilişkileri kurabilmektedirler.

Bu kapsamda, 5411 sayılı Kanunun 73 üncü maddesinin üçüncü fıkrasında öngörülen *"... müşteri sırrı niteliğindeki bilgiler, ..."* müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz." hükmü ile 5411 sayılı Kanunun anılan maddesine dayanılarak hazırlanmış Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmeliğin ilgili hükümleri çerçevesinde iş ortaklarına kişisel veri aktarımı gerçekleştirilebilecektir.

2- Yurtdışına Veri Aktarımı
2.1. Yurtdışına Veri Aktarımı Yöntemleri

Kanunun kişisel verilerin yurt dışına aktarılmasına ilişkin usul ve esasları düzenleyen 9 uncu maddesinin;

a) birinci fıkrasında, Kanunun 5 inci ve 6 ncı maddelerinde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması,
b) dördüncü fıkrasında, yeterlilik kararının bulunmaması durumunda, Kanunun 5 inci ve 6 ncı maddelerinde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, anılan fıkrada belirtilen uygun güvencelerden birinin taraflarca sağlanması ve
c) altıncı fıkrasında ise yeterlilik kararının bulunmaması ve dördüncü fıkrada öngörülen uygun güvencelerden herhangi birinin sağlanamaması durumunda, arızi olmak kaydıyla sadece bahse konu altıncı fıkrada belirtilen istisnai hâllerden birinin varlığı

hâlinde kişisel verilerin yurt dışına aktarılabileceği hükme bağlanmıştır.

Diğer taraftan, anılan maddenin onuncu fıkrasında kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlenmiştir. Yine, Anayasanın 90 ıncı maddesinin beşinci fıkrasında, "Usulüne göre yürürlüğe konulmuş milletlerarası andlaşmalar kanun hükmündedir. (...)" denilmek suretiyle uluslararası andlaşmaların usulüne uygun olarak iç hukukumuza dâhil edilmesi halinde kanun hükmünde sayılacağı açıkça düzenlenmiştir. Dolayısıyla, kanunlarda ve usulüne göre yürürlüğe konulmuş uluslararası andlaşmalarda kişisel verilerin yurt dışına aktarımına ilişkin özel bir düzenlemenin mevcut olması hâlinde, kişisel verilerin yurt dışına aktarılması faaliyetinin bu hükümlere uygun olarak gerçekleştirilmesi gerekecektir.

Bu çerçevede 5411 sayılı Bankacılık Kanunun "Sırların saklanması" başlıklı 73 üncü maddesinin Kanunun 9 uncu maddesinin onuncu fıkrası kapsamında değerlendirilmesi marifetiyle gerçekleştirilecek yurtdışına veri aktarımları bakımından dikkate alınması gerekmektedir. 04.06.2021 tarihli ve 31501 sayılı Resmi Gazetede yayımlanan Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik ile müşteri sırrı niteliğindeki bilgilerin paylaşım ve aktarımlarına ilişkin kapsam, şekil, usul ve esasları belirlenmiştir. Dolayısıyla, 6698 sayılı Kanunun gerek 4 üncü maddesinin birinci fıkrasında yer verilen "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." gerek 9 uncu maddesinin onuncu fıkrasında öngörülen "Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükümleri uyarınca müşteri sırrı niteliğindeki kişisel verilerin yurt dışına aktarımı bakımından 5411 sayılı Kanunda öngörülen mezkûr düzenleme ile anılan Yönetmelik hükümlerinin göz önünde bulundurulması gerekmektedir.

2.1.1. Yeterlilik Kararı

Kanunun kişisel verilerin yurt dışına aktarılmasına ilişkin usul ve esasları düzenleyen 9 uncu maddesinin birinci fıkrasında, Kanunun 5 inci ve 6 ncı maddelerinde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması hâlinde kişisel verilerin yurt dışına aktarılabileceği hükme bağlanmıştır.

Maddenin yeni düzenlemesi ile önceki düzenlemede değişiklik yapılarak, bu yeterlilik kararının sadece bir ülkenin geneli için değil, o ülkenin belirli bir sektörü veya uluslararası kuruluşlar için de verilebilmesine olanak sağlanmıştır. Bu bağlamda, gerekli şartların sağlanması durumunda Bankacılık sektörü bakımından yeterlilik kararı alınabilmesi mümkündür.

2.1.2. Uygun Güvenceler

Kanunun kişisel verilerin yurt dışına aktarılmasına ilişkin usul ve esasları düzenleyen 9 uncu maddesinin dördüncü fıkrasında, yeterlilik kararının

bulunmaması durumunda, Kanunun 5 inci ve 6 ncı maddelerinde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, anılan fıkrada belirtilen uygun güvencelerden birinin taraflarca sağlanması hâlinde kişisel verilerin yurt dışına aktarılabileceği hükme bağlanmıştır.

Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları arasında uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı + Kurul izni.

Dördüncü fıkranın (a) bendine göre yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurulun aktarıma izin vermesi koşullarının gerçekleşmesiyle yurtdışına veri aktarımı gerçekleştirilebilecektir. Buna istinaden, ülkemizdeki bir kamu kurumunun yabancı ülkedeki ilgili kamu kurumuyla belli alanda yapacağı iş birliği protokolü çerçevesinde, Kurulun izin vermesi koşuluyla, bu iş birliği kapsamındaki faaliyetlerin gerektirdiği kişisel verilerin yurt dışındaki kamu kurumuna aktarılması mümkün hale gelecektir.

Kurul tarafından Onaylanmış Bağlayıcı Şirket Kurallarının varlığı

Dördüncü fıkrada yer alan (b) bendine göre, aynı teşebbüs grubu içinde bulunan şirketler arasında, Kurul tarafından önceden onaylanmış ve kişisel verilerin korunmasını içeren bağlayıcı şirket kurallarının bulunması durumunda, Kanunun 5 ve 6 ncı maddelerindeki veri işleme şartlarından biri de mevcut ise, Kuruldan ek bir izin alınmadan bu şirketler arası veri aktarımı gerçekleştirilebilecektir. Böylece Kurulca onaylanan bağlayıcı şirket kuralları olan bir teşebbüs grubunun Türkiye'deki şirketinden, aynı grubun yabancı ülkedeki şirketine Kuruldan bir kez daha izin alınmaksızın veri aktarımı yapılabilecektir.

Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler,

özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmelerin varlığı + Kurula bildirim.

Dördüncü fıkrada belirtilen (c) bendine göre, Kurul tarafından yayımlanan standart sözleşmenin imzalanması, ek bir izin gerektirmeden veri aktarımına olanak tanıyacaktır. Bu standart sözleşme ise; veri kategorileri, aktarımın amaçları, verilerin alıcıları ve alıcı grupları, veri alıcısı tarafından uygulanacak teknik ve idari önlemler, özel nitelikli kişisel veriler için alınacak ek tedbirler gibi çeşitli önemli unsurlar ile hususları içermektedir.

Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı + Kurul izni.

Dördüncü fıkrada yer alan (ç) bendi uyarınca sektörel ya da bölgesel zorunluluklar sebebiyle standart taahhütname ile yurt dışına kişisel veri aktarımını gerçekleştiremeyecek aktarım taraflarının, aralarında yapacakları kişisel verilerin korunmasına ilişkin taahhütleri içeren taahhütnameyi Kurulun onayına sunmaları sonucu kişisel veri aktarımı gerçekleştirilebilecektir.

2.1.3. Arızi Haller

Kanunun 9 uncu maddesinin altıncı fıkrası ve Yönetmeliğin 6 ncı maddesinin ikinci fıkrası ile 16 ncı maddesinin birinci fıkrasında yer verildiği üzere veri sorumluları ve veri işleyenler, yeterlilik kararının bulunmaması ve uygun güvencelerden herhangi birinin de sağlanamaması durumunda arızi olmak kaydıyla yurtdışına kişisel veri aktarabilir. Ancak, arızi aktarım, sadece Kanunun 9 uncu maddesinin altıncı fıkrası ve Yönetmeliğin 16 ncı maddesinin ikinci fıkrasında sayılan hallerden birinin varlığı halinde mümkündür. Bu haller;

a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.
b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.
ç) Aktarımın üstün bir kamu yararı için zorunlu olması.
d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.
e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.
f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması." şeklinde, maddenin lafzından da anlaşılacağı üzere sınırlayıcı biçimde sayılmaktadır.

Aktarım yapılacak ülkede yeterli koruma bulunduğuna ilişkin bir Kurul kararı veya aktarım taraflarınca sağlanan herhangi bir uygun güvence bulunmadığı için yurt dışına kişisel veri aktarımı yapılamadığı; ancak yurt dışına kişisel veri aktarımı yapılmasının elzem olduğu durumlar için istisnalar öngörülmüştür. Anayasanın 20 nci maddesinin üçüncü fıkrasında bir temel hak ve özgürlük olarak tanınan kişisel verilerin korunmasını isteme hakkından bireylerin en üst düzeyde ve en geniş kapsamda yararlanabilmeleri için bu istisnai hallerin dar yorumlanması gerekmektedir. Ayrıca, bu kapsamda öngörülen istisna hallerinin arızi, düzenli olmayan, süreklilik göstermeyen ve nadiren gerçekleşen aktarım faaliyetleri bakımından geçerli olacağı açıkça düzenlenmiştir.

Bankalar açısından mümkün olabilecek arızi hallere örnekler:

Türkiye'de kurulu "A" bankasının, para gönderme talebini karşılamak üzere ilgili müşterinin kişisel verilerini Etiyopya'da kurulu "B" bankasına göndermesi ilgili kişinin bir yeterlilik kararının ve uygun güvencelerin yokluğundan ötürü doğacak risklere ilişkin muhakkak bilgilendirilmesinden sonra açık rızasına başvurularak, aktarımın düzenli olmaması, süreklilik

göstermemesi ve nadiren gerçekleşmesi ve Bankanın mutat işlemleri arasında yer almaması kaydıyla gerçekleştirilebilecektir.

Bir Banka tarafından dava sürecini yürütmek amacıyla kişisel verilerin yurt dışına aktarılması bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması arızi haline dayanılarak aktarımın düzenli olmaması, süreklilik göstermemesi ve nadiren gerçekleşmesi kaydıyla gerçekleştirilebilecektir.

2.1.4. Kanunun 9 uncu Maddesinin Onuncu Fıkrası Uyarınca Yapılacak Aktarımlar

Kanunun "Kişisel Verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesinin onuncu fıkrasında kişisel verilerin yurt dışına aktarılması ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlenmiştir.

09/04/2020 tarihli ve 2020/265 sayılı Kurul Kararı'nda Kanunun 9 uncu maddesinin onuncu fıkrasına göre diğer kanunlarda yurt dışına veri aktarımına ilişkin özel hükümlerin varlığı halinde; bu hükümlerin öncelikli olarak uygulanacağı, 20/02/2020 tarihli ve 7222 sayılı Bankacılık Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunun 10 uncu maddesinin gerekçesinde de ifade edildiği üzere, esasen kişisel verilerin bankacılık hukukunda özel bir görünümü olan gerçek kişi müşteri sırları (müşteri bilgileri) bakımından 5411 sayılı Kanunun hükümlerinin, 6698 sayılı Kanuna göre özel hüküm niteliğini haiz bulunmakta olduğu ve özel norm-genel norm ilişkisinde özel normların uygulama alanı bulacağı ifade edilmiştir. Bir başka ifadeyle, banka ya da müşteri sırrının paylaşımının sır saklama yükümlülüğünün dışında olduğu durumların düzenleme altına alındığı söz konusu hükmün, belirli koşullar altında banka ya da müşteri sırrının paylaşılmasına cevaz veren, bu nitelikteki kişisel verilerin aktarımına ilişkin özel bir düzenleme niteliğini haiz olduğu belirtilmiştir. Müşteri sırrı, 5411 sayılı Bankacılık Kanununun 73 üncü maddesinin üçüncü fıkrasında "Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler" olarak tanımlanmıştır.

Bir gerçek veya tüzel kişi müşterinin, bankanın müşterisi olduğunu gösterir her türlü bilgi müşteri sırrı olarak kabul edilmektedir. Bununla birlikte, Yönetmeliğin 4'üncü maddesinin üçüncü fıkrasında müşteri ilişkisi kurulmamış olsa dahi, başka bir banka nezdinde bulunan müşteri sırrı niteliğindeki bilgilerin diğer bir banka tarafından elde edilmesi ve öğrenilmesi halinde, bu verilerin de diğer banka için müşteri sırrı niteliğini haiz olacağı öngörülmüştür. Bu anlamda, bankalar ile müşteri ilişkisi kurulmadan önce de var olan ve başka bir bankanın müşteri sırrı niteliğinde olmayan gerçek kişilere ait kişisel veriler tek başına müşteri sırrı olarak kabul edilmemektedir. Ancak bu nitelikteki kişisel verilerin, ilgili gerçek kişinin banka müşterisi olduğunu gösterecek şekilde tek başına ya da müşteri ilişkisinin kurulmasından sonra oluşan verilerle birlikte işlendiğinde müşteri sırrı haline gelecektir.

Bu kapsamda, 5411 sayılı Kanunun 73 üncü maddesinin dördüncü fıkrasında belirtilen sınırlar dâhilinde banka sırrı ya da müşteri sırrı niteliğini haiz kişisel verilerin yurtdışına aktarımı Kanunun 9 uncu maddesinin onuncu fıkrasına dayanılarak gerçekleştirilebilecektir. Ancak her ne kadar 6698 sayılı Kanunun 9 uncu maddesinin onuncu fıkrası uyarınca 5411 sayılı Kanunun 73 üncü maddesinin dördüncü fıkrası çerçevesinde kişisel veri aktarımı gerçekleştirilebilecek olsa da söz konusu aktarımlar bakımından Kanunun diğer hükümlerine uygun davranılması gerekliliği devam etmektedir. Özellikle Kanunun 4 üncü maddesinde düzenlenen genel ilkelere riayet edilmesi ve 12 nci maddesi uyarınca gerekli idari ve teknik tedbirlerin alınması gerekmektedir.

Anılan karar gereği; özetle, 5411 sayılı Bankacılık Kanunu'nun 73 üncü maddesi, 5411 sayılı Bankacılık Kanunu'nun 73 ve 93 üncü maddelerine dayanılarak hazırlanan Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik ve müşteri sırrının paylaşımının düzenlendiği ilgili diğer mevzuata uygun şekilde müşteri sırrı niteliğini haiz kişisel veriler yurt dışına aktarılabilecektir.

IX. Genel İlkeler

6698 sayılı Kanunun "Genel ilkeler" başlıklı 4 üncü maddesinde, kişisel verilerin ancak anılan Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; *"-Hukuka ve dürüstlük kurallarına uygun olma, -Doğru ve gerektiğinde güncel olma, -Belirli, açık ve meşru amaçlar için işlenme, -İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, -İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."* şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına alınmıştır. Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta 6698 sayılı Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulması hukuki bir gerekliliktir.

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

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

Genel ilkelerden kişisel verilerin "belirli, açık ve meşru amaçlar için işlenme" ilkesi ise, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliği sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Bir diğer önemli ilke olan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması" ilkesine göre, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, amaç için gerekli olmayan veri işlemeden kaçınılmasıdır. Ölçülülük ilkesi ise, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani veri işlemenin, amacı gerçekleştirecek ölçüde olması demektir. Söz konusu ilkeler çerçevesinde Kişisel Verileri Koruma Kurulunun 18/09/2019 tarihli ve 2019/277 sayılı kararı ile "(...) Şikâyetçinin müşterisi olduğu Bankaya kendisine ait iş ve işlemlerde ulaşılması adına vermiş olduğu telefon numarası bilgisinin, eşine ulaşılmasında yardımcı olunabilmesi adına işlenmesinin, 5598 sayılı Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (c) ve (ç) bentlerinde yer alan kişisel verilerin işlenmesinde "belirli, açık ve meşru amaçlar için işlenme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uyulması zorunluluğuna aykırı olduğu ve bu çerçevede Kanunun 12 nci maddesinin birinci fıkrasının (a) bendi uyarınca veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığını göstermesi nedeniyle Banka hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına" karar verilmiştir.[46]

[46] "Bir bankanın, ilgili kişinin cep telefonu numarasını bankaya veriliş amacı dışında kullanması" hakkında Kişisel Verileri Koruma Kurulunun 18/09/2019 Tarihli ve 2019/277 Sayılı Karar Özeti, www.kvkk.gov.tr

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

X. Veri Sorumlusunun Yükümlülükleri

A. Aydınlatma Yükümlülüğü

Veri sorumlusunun aydınlatma yükümlülüğü, 6698 sayılı Kanun'un 10'uncu maddesinde ve 10 Mart 2018 tarih, 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğ'de düzenlenmiştir. Bu yükümlülük kapsamında, veri sorumlusu tarafından kanunda öngörülen hukuka uygunluk nedenlerine dayalı olarak kişisel veri işlendiği her durumda uygun kanallar ve anlaşılır, açık ve sade bir dil kullanılarak aşağıdaki konu başlıklarında ayrıntılı olarak yer verildiği şekilde ilgili kişilere aydınlatma yapılır.

1- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde İçerik

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 10'uncu maddesi uyarınca kişisel verilerin elde edilmesi sırasında veri sorumluları; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, Kanun'un 11'inci maddesinde sayılan diğer hakları konusunda bilgi vermekle yükümlüdür.

Her banka, kişisel veri kategorileri, veri toplama yöntemi, işleme amaçları ve hukuki gerekçeleri ile kişisel verilerin aktarıldığı taraflar kapsamında, kendi işleyiş ve sistemlerine uygun olarak kendi aydınlatma metinlerini oluşturabilecektir.

Diğer taraftan aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Veri Sorumluları Sicil Bilgi Sistemi'nde (VERBİS) açıklanan bilgilerle uyumlu olmalıdır.

Kişisel Verileri Koruma Kurumu tarafından yayımlanan 26/06/2020 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu

Duyurusu'nda[47] ve Kişisel Verileri Koruma Kurulu'nun 08/10/2020 tarih, 2020/765 sayılı[48] ve 766 sayılı kararlarında[49], bankalarca yapılacak aydınlatmaların, kişisel veri işleme faaliyetine özgülenmiş olarak yerine getirilmesi gerektiği açıkça ifade edilmiştir.

Bu kapsamda, 5411 sayılı Bankacılık Kanunu'nun 4 üncü maddesinde[50] yer alan bankacılık faaliyet konuları aşağıda sıralanan başlıklar altında toplanmıştır:

[47] Duyurunun tam metni için bkz. https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU

[48] Kararın tam metni için bkz. https://www.kvkk.gov.tr/Icerik/6844/2020-765

[49] Kararın tam metni için bkz. https://www.kvkk.gov.tr/Icerik/6849/2020-766

[50] Bankacılık Kanunu'nun "Faaliyet konuları" başlıklı 4. madde düzenlemesi:

"Bankalar, diğer kanunlarda öngörülen hükümler saklı kalmak kaydıyla aşağıda belirtilen faaliyetleri gerçekleştirebilirler:

a) *Mevduat kabulü.*

b) *Katılım fonu kabulü.*

c) *Nakdî, gayrinakdî her cins ve surette kredi verme işlemleri.*

d) *Nakdî ve kaydî ödeme ve fon transferi işlemleri, muhabir bankacılık veya çek hesaplarının kullanılması dahil her türlü ödeme ve tahsilat işlemleri.*

e) *Çek ve diğer kambiyo senetlerinin iştirası işlemleri.*

f) *Saklama hizmetleri.*

g) *Kredi kartları, banka kartları ve seyahat çekleri gibi ödeme vasıtalarının ihracı ve bunlarla ilgili faaliyetlerin yürütülmesi işlemleri.*

h) *Efektif dahil kambiyo işlemleri; para piyasası araçlarının alım ve satımı; kıymetli maden ve taşların alımı, satımı veya bunların emanete alınması işlemleri.*

i) *Ekonomik ve finansal göstergelere, sermaye piyasası araçlarına, mala, kıymetli madenlere ve dövize dayalı; vadeli işlem sözleşmelerinin, opsiyon sözleşmelerinin, birden fazla türev aracı içeren basit veya karmaşık yapıdaki finansal araçların alımı, satımı ve aracılık işlemleri.*

j) *Sermaye piyasası araçlarının alım ve satımı ile geri alım veya tekrar satım taahhüdü işlemleri.*

k) *Sermaye piyasası araçlarının ihraç veya halka arz yoluyla satışına aracılık işlemleri.*

l) *Daha önce ihraç edilmiş olan sermaye piyasası araçlarının aracılık maksadıyla alım satımının yürütülmesi işlemleri.*

m) *Başkaları lehine teminat, garanti ve sair yükümlülüklerin üstlenilmesi işlemleri gibi garanti işleri.*

n) *Yatırım danışmanlığı işlemleri.*

o) *Portföy işletmeciliği ve yönetimi.*

p) *Hazine Müsteşarlığı ve/veya Merkez Bankası ve kuruluş birlikleri nezdinde oluşturulan bir sözleşme kapsamında üstlenilen yükümlülükler çerçevesinde alım satım işlemlerine ilişkin piyasa yapıcılığı.*

r) *Faktöring ve forfaiting işlemleri.*

s) *Bankalararası piyasada para alım satımı işlemlerine aracılık.*

t) *Finansal kiralama işlemleri.*

u) *Sigorta acenteliği ve bireysel emeklilik aracılık hizmetleri.*

v) *Kurulca belirlenecek diğer faaliyetler.*

Mevduat bankaları birinci fıkranın (b) ve (t), katılım bankaları (a), kalkınma ve yatırım bankaları (a) ve (b) bentlerinde belirtilen faaliyetleri gerçekleştiremezler."

1) Müşteri Edinimi/Hesap Açılış
2) Kredi
3) Yatırım İşlemleri

Bankanın veri işleme amaçlarının çok sayıda olması sebebiyle, yukarıda açıklanan kapsamda aydınlatma metinlerinin Bankalarca hazırlanması uygun olacaktır. Bankalarca, kendilerine başvuruda bulunan ilgili kişiye bankaya geliş amacına göre, faaliyete özgülenmiş aydınlatma yapılması müşteri olmayan kişilerin banka ile sürekli iş ilişkisi kurmaması durumunda sürecin, faaliyete özgülenmiş aydınlatma ile son bulması uygun olabilecektir.

Örneğin, kişi tüketici kredisi/kredi kartı başvurusunda bulunduğunda krediye özgü aydınlatma yapılacak, kredi reddedilir ve kişi, banka müşterisi haline gelmez ise süreç sonlanmış olacaktır.

İlgili kişinin banka müşterisi haline gelmesi durumunda ise banka tarafından bu kişiye "Müşteri Edinimi/Hesap Açılışı" için hazırlanan aydınlatma metni içeriğiyle uyumlu bir bilgilendirme yapılması uygun olacaktır.

Faaliyet başlıkları içerisinde mevcut "hesap açılış" konusunda ise, bankaya müşteri olmak için başvuran kişilere "Müşteri Edinimi/Hesap Açılışı" için düzenlenecek bir metin ile aydınlatma yapılması uygun olabilecektir. Zira, ilgili kişi müşteri olarak edinilmekte, sürekli iş ilişkisi kurulduktan sonra ise ancak talebi olması halinde kendisine farklı ürünler tahsis edilmektedir. Bazı ürün tahsislerinde müşteri edinim aşamasında elde edilen kişisel veriler dışında başka bir veri işleme faaliyeti olmadığından, yapılacak bu aydınlatma yeterli olabilecektir. Örneğin, kiralık kasa tahsis edilirken müşterinin sadece kimlik ve iletişim bilgileri işlenmektedir.

Bankalarca yukarıda açıklanan kriterlere uygun şekilde hazırlanacak olan aydınlatma metinlerinde kişisel verilerin kategorik bazda işleme amaçları ve hukuki sebepler ile eşleştirilerek sunulması gerektiğine dikkat edilmelidir.

Kişisel verilerin kimlere aktarılabileceğine yönelik zorunlu içerikte de; destek hizmeti alınan kuruluşlar, iş ortakları, iştirakler, denetim kuruluşları,

yetkili kamu kuruluşları vs. gibi üçüncü kişi gruplarına kategorik olarak yer verilebilecek ve bazı kurumların sayılması da tercih edilebilecektir.

Kanun'da belirtildiği üzere "veri sorumlusu" olarak bankalar, verisini işledikleri gerçek kişileri (personel, ziyaretçi vb.) aydınlatmakla yükümlüdür. Aydınlatma, aşağıda belirtilen kanallar aracılığı ile yapılmaktadır.

Bankacılık faaliyetleri kapsamında bankaların ilgili kişilere yapmış oldukları bilgilendirme dışında kalan durumlarda da kişisel verilerin elde edildiği aşamalarda ilgili kişiye, amaca uygun ilave bir bilgilendirme yapılması önerilmektedir. Örneğin, kimlik doğrulamada biyometrik verilerin kullanılması ya da geniş kitleleri etkileyebilecek ve yeni teknolojilerin kullanıldığı ürün/süreçlerde veya yarışma/çekilişlere katılım gibi hususlarda somut duruma özgülenmiş aydınlatma yapılabilir.

1.1. Katmanlı Aydınlatma

Katmanlı aydınlatma, kişisel verilerin elde edilmesi sırasında ilgili kişiye, kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin Kanunun 10. maddesine uygun aydınlatmaya yönlendirilmesi[51] amaca ilişkin bilgilendirilme yapılırken, önce kısa ve kolay anlaşılır bir metin sunup, eş zamanlı (just-in-time) metin vasıtasıyla, detaylı açıklamalara işaret edilmesi/referans verilmesi durumudur.

Zaman ve yer kısıtı olan kanallarda, ilgili kişiye doğrudan aydınlatma metninin gösterilmesinin ya da okunmasının mümkün olmadığı durumlarda, katmanlı aydınlatma yapılması yeterli olabilir. Bu bağlamda bankalarca sunulan ürün ve hizmetlerin çeşitliliği göz önüne alındığında; banka ile müşteri arasında gerek yüz yüze, gerekse elektronik araçlarla sözleşme kurulması sırasında, müşterinin tüm aydınlatma metnini okumasının elverişli olmadığı durumlarda aydınlatma yükümlülüğü, ilgili kişilere kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak Bankaların internet sitelerinde yer alan ve Kanun'un 10'uncu maddesine uygun şekilde düzenlenmiş

[51] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s.8. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf)

aydınlatma metinlerine yönlendirme yapılarak yerine getirilebilecektir. Bununla birlikte, katmanlı aydınlatma yöntemi tercih ediliyorsa, ilgili kişilerin ayrıntılı bilgi için başka bir mecraya yönlendirilmesinden önce, ilk aşamada temel bilgilerin (örneğin veri sorumlusunun kimliği ve veri işlemenin amacı) sunulduğundan emin olunmalı, yönlendirilen metinlerin işleme faaliyeti ile sınırlı içeriğe sahip olduğuna dikkat edilmelidir.[52]

Bu duruma uyan başlıca örnekler, online (çevrimiçi) bir formun doldurulması suretiyle veri toplanması sırasında verinin toplandığı yerler, güvenlik kamerası barındıran yerler, çağrı merkezleri veya benzeri ses kayıt barındıran sistemler, internet veya mobil bankacılık ara yüzleri, ATM'ler veya SMS kanalıyla bilgilendirmede kullanılabilecek karakter sayısının izin verdiği ölçüde yapılan açıklama dışında ilgili kişinin banka internet sitesinde yer alan aydınlatma metinlerine yönlendirilmesi olarak sayılabilir.

Bu örneklere ek olarak; bina içi ve dışına ilişkin görüntü kaydının alındığı yerlerde, giriş kapısı veya yakınında, aşağıdaki unsurları taşıyan bir işaretin bulundurulması, aydınlatma için yeterli olabilir:

- Makul bir uzaklıktan rahatça ne olduğu anlaşılabilecek büyüklükte bir kamera simgesi
- Okunmaya elverişli boyutta olacak şekilde, örneğin "Bu bina içi ve etrafında güvenlik kameraları ile kayıt alınmaktadır' benzeri bir ifade
- Okunmaya elverişli boyutta olacak şekilde, örneğin "Kişisel Verilerin Korunması Kanunu ve haklarınız hakkında daha detaylı bilgiyi bankamız internet sitesinden edinebilirsiniz http://www.banka.com.tr' benzeri bir ifade (veya tercihen karekod vb. yönlendiriciler)

Bankacılık sektöründe tüm veri işleme amaçlarının müşterilere sağlıklı ve yönetilebilir bir şekilde aktarılmasında katmanlı aydınlatma yönteminin kullanılması benimsenebilir.

[52] https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU

2- Aydınlatma Yükümlülüğünün Yerine Getirilme Zamanı

Aydınlatma yükümlülüğünün kural olarak veri sorumlusu tarafından kişisel verinin elde edilmesi aşamasında yerine getirilmesi gerekmektedir.

Ancak; veri sorumlusu tarafından kişisel verilerin ilgili kişiden elde edilmemesi halinde; veri sorumlusu tarafından ilgili kişiyi aydınlatma yükümlülüğü kişisel verinin elde edilmesi aşamasından sonra yerine getirilebilir. Örneğin maaş ödemelerinde; maaş ödemesi yapılacak firmadan çalışanların kişisel verilerinin temin edilmesi halinde çalışanların aydınlatılmaları durumlarında. Bu halde aydınlatma yükümlülüğünün;

-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

yerine getirilmesi gerekmektedir.

3- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Usul

Aydınlatma yükümlülüğünün yerine getirilmesindeki usul yasal olarak herhangi bir şekil şartına bağlanmadığı gibi ilgili kişinin talebine veya onayına da tabi tutulmamıştır. Dolayısıyla veri sorumluları aydınlatma yükümlülüklerini sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yerine getirebilir. Ancak aydınlatma yükümlülüğünün yerine getirildiği yönündeki iddiada ispat külfeti veri sorumlusu üzerinde olduğundan aydınlatma yükümlülüğünün ispata elverişli kanallardan yerine getirilmesi önem arz etmektedir.

Kişisel veri işleme amacı değişmediği sürece, aydınlatma yükümlülüğünün yerine getirilmesinde kullanılacak kanallar arasından herhangi bir kanal vasıtasıyla ilgili kişinin aydınlatılması sağlanır.

Bankacılık sektörü açısından aydınlatma aşağıda belirtilen kanallar aracılığı ile yapılabilmektedir.

3.1. Şube

Şubelerin, müşteriler başta olmak üzere bankacılık faaliyetlerinin tarafı olan ilgili kişilerle yüz yüze temasın gerçekleştirildiği temel kanal olması nedeniyle, aydınlatma yükümlülüğünün şubeler aracılığı ile yerine getirilmesi mümkündür. Aydınlatma yükümlülüğünün şubeler kanalı ile gerçekleştirilmesine yönelik iyi uygulama örneklerine aşağıda yer verilmiştir. Şubelerde Kanun'a uygun aydınlatma yükümlülüğünün yerine getirilmesinde ilgili kişinin bilgi sahibi olacağı şekilde görsel veya basılı ortamda (afiş, broşür, pano, dijital ekran vb.) aydınlatma yapılabilir.

şubelerde aydınlatma metni ilgili kişiye teslim edilebilir. Bunun yanı sıra yine Şubede işlem sırasında aşağıda belirtilen yöntemlerle de aydınlatma yapılmasının önünde bir engel bulunmamaktadır.

3.2. İnternet Sitesi

Bankaların internet sitelerinde, Bankanın aydınlatma metinlerine kolayca ulaşılabilir şekilde yer verilmesi önerilmektedir. Böylelikle, katmanlı aydınlatmalarda verilen linkler vasıtasıyla bu metinlere yönlendirilen müşterilere kolayca aydınlatma, bankalar açısından da aydınlatma yükümlülüğünün yerine getirilmesi imkânı sağlanabilecektir.

İşleme faaliyeti ile sınırlı olmayan, veri sorumlusu için genel veri işleme belgesi niteliğinde olan gizlilik politikaları veya veri işleme politikaları, aydınlatma metinleri olarak kullanılmamalıdır.[53]

[53] https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU

3.3. İnternet Şube

İnternet şube kullanıcıları, internet şube aracılığıyla karşılarına çıkartılacak olan aydınlatma metinleri aracılığıyla bilgilendirebilir.

3.4. Mobil Şube ve Mobil Uygulama

Mobil şube/uygulama kullanıcıları, mobil şube/uygulama aracılığıyla karşılarına çıkartılacak olan aydınlatma metinleri ile bilgilendirebilir.

İlgili kişilere anlık bildirim (push notification) ile aydınlatma metni gönderilmesi ve yine kısa ve yönlendirici bir aydınlatma metni ile aydınlatma yükümlülüğü yerine getirebilir.

3.5. Çağrı Merkezi/IVR

İlgili kişiye görüşmenin başında bir tuşa basma seçeneği sağlanarak aydınlatma metnini dinlemek isteyenlere aşağıdaki örnek metin sunulabilir.

Örnek Çağrı Merkezi Metni:

"Kişisel verilerinizin ne şekilde işlendiğine dair aydınlatma metnini dinlemek için 1'e, daha önce bu konuda bilgilendirildiyseniz, dinlemeden ilerlemek için 2'ye basınız." Bu örnek metnin ifadeleri bağlayıcı olmamakla birlikte, yöntemi göstermek amacıyla belirtilmiştir.

Yukarıdaki örneğe uygun olacak şekilde, 1'e basarak metni dinlemeye karar veren kişilere dinletilecek ses kaydında, metnin tamamının ilgili kişiye dinletilmesinin öncesinde bu metinlerin erişilebileceği diğer ortamların ifade edilmesi halinde, bu ifade okunduktan sonra bağlantının kesilmesi ya da ilgili kişinin telefonu kapatması durumlarında da veri sorumlusu banka, aydınlatma yükümlülüğünü yerine getirmiş olur.

Yukarıdaki örneğe uygun olacak şekilde, 2'ye basarak metni dinlememeye karar veren kişiler yönünden aydınlatma yükümlülüğü yerine getirilmiş olur.

3.6. Elektronik Posta

İlgili kişilerin bankaya iletişime geçmek üzere verdikleri elektronik posta adreslerine (örneğin hesap özetlerinin, kredi kartı ekstrelerinin gönderildiği adresleri) veya elektronik tebligat adreslerine iletilecek aydınlatma metinleri ile bilgilendirme yapılabilir.

3.7. Fiziki Posta

İlgili kişi tarafından bankalara iletişim/tebligat adresi olarak bildirilen adrese aydınlatma metninin gönderilmesi (örneğin, kredi kartı hesap özeti ile aynı zarfta gönderilmesi) ile bilgilendirme yapılabilir.

3.8. SMS

SMS kanalıyla yapılan aydınlatmalarda, kanalın izin verdiği uzunlukta bir metne ve tıklandığında aydınlatma metnine yönlendiren bir linke yer verilerek katmanlı aydınlatma yapılabilir.

Örnek SMS Metni

"..... tarafından hazırlanan kişisel verilerinizin işlenme ve aktarılma amacı, toplanma yöntemi, hukuki sebep ve haklarınıza ilişkin aydınlatma metnine ulaşmak için <link> tıklayınız."

3.9. ATM

Kısa Mesaj Servisi (SMS) gibi sınırlı karakter girilebilen bir alan olan ATM kanalından yapılan bilgilendirmelerde, kısa bir metne yer verildikten sonra ilgili kişinin aydınlatma metnine erişebileceği şekilde katmanlı aydınlatma yapılması mümkündür.

Örnek ATM Metni

"..... tarafından hazırlanan kişisel verilerinizin işlenme ve aktarılma amacı, toplanma yöntemi, hukuki sebep ve haklarınıza ilişkin aydınlatma metnine ulaşmak için buton/menü'yü tıklayabilirsiniz/ metne ... linkinden(*) ulaşabilirsiniz."

(*) Ekran tasarımlarına göre bankalarca tercih edilecek ifadeye yer verilebilecektir

4- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Özel Durumlar
4.1. İmza Yetkilileri ve Gerçek Faydalanıcıların Aydınlatılması

Tüzel kişileri temsile yetkili gerçek kişilerin temsil yetkilerinin tevsik edilmesi amacıyla ibraz edilen belgelerde, bu gerçek kişilerin kişisel verileri yer almakta ve bu veriler tüzel kişiyi temsile yetkili kişilerin belirlenmesi amacıyla işlenmektedir. Ticari hayatın doğal akışı içinde, bir tüzel kişiyi temsile yetkili gerçek kişinin, temsile yetkili olduğu tüzel kişinin ilgili belgelerinde kişisel verilerinin bulunduğu ve bu belgelerin söz konusu yetkilendirmeyi tevsik amacıyla ilgili kurum ve kuruluşlara aktarılacağı ve bu kuruluşlar tarafından bu amaçla işleneceğine ilişkin aydınlatma yükümlülüğü temsilciyi atayan tüzel kişidedir.

Dolayısıyla, tüzel kişileri temsile yetkili gerçek kişilerin hali hazırda, söz konusu işleme amacı yönünden kişisel verilerinin Banka'ya aktarılacağı hususunda tüzel kişi tarafından bilgilendirildikleri göz önüne alınarak, verilerin aktarıldığı kurum ve kuruluşların (bankaların) bu amaçla sınırlı olarak gerçekleştirilen veri işlemeleri yönünden, Aydınlatma Tebliği'nin 6'ncı maddesi kapsamında ayrıca bir aydınlatma yapılmasına gerek bulunmamaktadır.

4.2. Risk Grubu'ndakilerin Aydınlatılması

Risk Grubu'nda yer alan kişilerin aydınlatılmasına ilişkin olarak; Kurul'un 26/07/2018 tarihli ve 2018/92 sayılı Kararı ile, bankalarca, 5411 sayılı Bankacılık

Kanunu ve ilgili diğer mevzuat kapsamında, bankaların kredi kullandırım faaliyetlerinde kredi başvurusunda bulunan kişilerin "Risk Grubu"nda bulunan ilgili kişilerin kişisel verilerinin işlenmesi faaliyeti sınırları dahilinde, bir başka deyişle sadece bu faaliyet özelinde yerine getirilecek aydınlatma yükümlülüğünün, 5411 sayılı Kanunun 73'üncü ve 159'uncu maddeleri ile 5237 sayılı Türk Ceza Kanununun 239'uncu madde hükümleri dikkate alınmak suretiyle, her bir kredi kullandırım işlemi özelinde "risk grubu"nda bulunan ilgili kişilerin tek tek aydınlatılması suretiyle değil de, kolayca erişilebilecek şekilde ve sadece "Risk Grubu" faaliyetleri bakımından genel bir aydınlatma yapılabileceği kanaatine varılmıştır.

Kişisel Verileri Koruma Kurulu'nun ilgili kararı doğrultusunda bankalarca internet sitesi marifetiyle aydınlatma yapılabilecektir.

4.3. Varlığın Sahibi Dışındaki Kişilere İlişkin Kişisel Verilerin ve Çek-Senetlerde Son Ciranta Dışındaki Kişilerin Kişisel Verilerinin İşlenmesi

Teminat işlemlerinde, varlığın sahibi dışındaki gerçek kişilerin verilerinin de teminata alınan varlığın temel bilgileriyle bütünleşmiş bir şekilde banka uhdesine geçmesi mümkün olabilmektedir. Varlığın önceki (veya kimi durumda sonraki) sahibi, vekâletle yapılan işlemlerde vekil veya tapu sicilinde görevli memurlar ile Türk Borçlar Kanunu'nun ilgili hükümlerine göre kefaletin geçerli sayılabilmesi için aranan eşin rıza bilgisi ve benzeri durumlarda verileri işlenen kişilerin kişisel verileri bu kapsamdadır. Bu kapsamdaki veriler, teminata ilişkin bilgi ve belgelerin doğal ve zorunlu unsurları olduklarından ve olası ihtilaflarda delil olarak ileri sürüleceklerinden, maskelenmeleri de mümkün değildir.

Bu tip verilerin bankaca üzerinde analiz gerçekleştirilmeye uygun şekilde sınıflandırılmadığı (örneğin varlığın eski sahibine veya onay vermiş tapu sicil memuruna göre sorgulanamadığı) durumlarda bunun Kanun'da tanımlanmış "tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleme" kapsamındaki bir veri işleme faaliyeti olmadığı söylenebilecektir. işlemin Kanun kapsamında bir kişisel veri işleme faaliyeti olmaması nedeniyle

ve bankaların bu kişiler ile işlem anında bir teması bulunmadığından bankaların ilgili kişileri tespit edip aydınlatma yapması fiili olarak mümkün olmayıp hayatın olağan akışına aykırıdır. Dolayısıyla bankaların bu kişilere karşı herhangi bir aydınlatma yükümlülüğü bulunmadığı söylenebilecektir.

Yine, uygulamalarda bankalar tarafından, tahsilinde müşterilerine ait risklere mahsup edilmek üzere kambiyo senetleri tahsile veya bedelleri kredi borcuna mahsup edilmek üzere teminata alınabilmektedir. Bu gibi durumlarda, son ciranta dışındaki keşideci, ara ciranta, avalist vb. kişilerin isim, imza gibi verileri ilgili belgenin doğal ve zorunlu unsuru olduğundan elde edilmektedir. Ancak kambiyo senedinin başka bir veri sorumlusu tarafından Bankaya iletilmesi suretiyle ilgili kişilerin kişisel verilerinin Bankaya aktarılması halinde söz konusu kişisel verilerin Bankaya aktarılacağına dair aydınlatma yükümlülüğü aktaran veri sorumlusuna ait olacağından bu durumda Bankanın ayrıca ilgili kişiye aydınlatma yapması gerekmeyecektir. ilgili veriler olası ihtilaflarda delil olarak ileri sürüleceklerinden maskelenmeleri de mümkün değildir.

4.4. Maaş Ödeme Anlaşmaları

Bankalar maaş ödeme anlaşması yapmış oldukları kurumlardan, maaş ödemesi yapılacak olan kişilerin kimlik tespitini gerçekleştirmek amacıyla kişisel verilerini temin etmekte ve toplu hesap açılışı yapmaktadırlar. Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik'in 6'ncı maddesi kimlik tespitinde gerekli olan bilgilerin ne olduğunu sıralı olarak düzenlemekte, Mali Suçları Araştırma Kurulu Genel Tebliği (Sıra No: 5) toplu maaş hesap açılışlarında alınması gereken zorunlu bilgileri belirlemektedir. Bu kapsamda bankalar, müşteri ile yüz yüze gelmeden, maaş ödeme anlaşması gereğince, kimlik tespitine ilişkin gerçek kişilerin kişisel verilerini elde ederek veri kayıt sistemine kaydetmekte ve bu kişilere aydınlatma yapabilme imkânı bulunmamaktadır.

Bununla birlikte söz konusu kişisel verilerin ilgili kuruluştan bankalara aktarılmasında aydınlatma yükümlülüğünün veri sorumlusu sıfatını haiz kuruluşta olduğu, bu yükümlülüğü doğrudan yerine getirebileceği

gibi yetkilendirdiği kişi aracılığıyla da yerine getirebileceği göz önünde tutulmalıdır. Söz konusu kişisel verilerin elde edilmesinden sonraki süreçte ise bankacılık faaliyetlerine ilişkin aydınlatma yükümlülüğünün bankalarda olduğu açıktır. Bankalar yapılan toplu hesap açılışını takiben maaş müşterisi olacak kişiler ile akdettikleri hizmet sözleşmesi ile müşteri ilişkisi kurmaktadırlar. Bu durumda kişisel verilerin ilgili kişilerden elde edilmemesi durumu ve bankanın kişisel verileri işlemesinin 6698 sayılı Kanunun 5'inci maddesinin 2'nci fıkrasının (ç) bendinde yer alan hukuka uygunluk sebebine dayandığı göz önüne alındığında, bankanın veri kayıt sisteminde tuttuğu söz konusu kişisel veriler için 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 yükümlülüğünü yerine getirmesi gerekmektedir.

4.5. Kredi Kartları ve Banka Kartları İşlemleri

Bankalar başta 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu olmak üzere Bankacılık Kanunu ve ikincil mevzuatları kapsamında banka kartları ve kredi kartlarının çıkarılması ve kullanımına ilişkin hizmet vermektedir.

Bankalar ulusal ve uluslararası kartlı sistem kuruluşları ile yaptığı anlaşmalar ve ilgili mevzuatlar uyarınca kartların farklı banka cihazlarında kullanılmasına olanak sağlarlar. Bankalar kart sahibi müşterilerinin kartlarını farklı banka cihaz ve poslarında kullanmaları halinde hangi verilerinin üçüncü kurum ve kuruluşlara aktarılacağı konusunda aydınlatmakla yükümlüdürler. Bu hususta aydınlatılan kart sahiplerinin kartlarını başka banka cihaz ve poslarını kullanmaları halinde ikinci kez cihaz ve pos sahibi banka tarafından aydınlatılmalarına gerek bulunmamaktadır.

B. Veri Sorumluları Sicili, Sicile Kayıt ve Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 16'ncı maddesinde

kamuya açık bir veri sorumluları sicili tutulacağı belirtilmiştir.

Veri sorumlusu olan bankaların da Veri Sorumluları Sicili'ne kayıt yükümlülüğü mevcuttur. Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri
b) Kişisel verilerin hangi amaçla işleneceği
c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar
ç) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları
d) Yabancı ülkelere aktarımı öngörülen kişisel veriler
e) Kişisel veri güvenliğine ilişkin alınan tedbirler
f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre

30.12.2017'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik ("Yönetmelik") ile de, Veri Sorumluları Siciline yapılacak kayıtlara ilişkin usul ve esaslar belirlenmiştir.

Yönetmelik ile "kişisel veri işleme envanteri" tanımı getirilmiştir. Bu tanım, veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri ifade etmektedir.

Yasal yükümlülüklerinin yanı sıra "Veri Sorumlusu" veya "Veri işleyen" sıfatıyla veri işleyen bankalar, süreçlerindeki veri işlemenin amacını, ölçülülük gereksinimlerine uygunluğunu, süresini ve diğer ilgili şartlarını takip etmek ve düzenlemek amacıyla bir veri envanterine ihtiyaç duyar. Bu veri envanteri, uygun bir veri yönetimi aracı ile banka sorumluluğunda güncel olarak takip edilir.

Veri envanteri Veri Sorumluları Siciline yapılacak bildirime de temel olacak yeterli bilginin sağlanabilmesi için asgari olarak aşağıdaki kategorileri içerir;

- İşlenen veri kategorisi
- Veri işleme amaçları
- Veri alıcı grupları
- Veri saklama süreleri
- Veri konusu kişi grupları
- Verinin aktarıldığı ülkeler
- Veri koruma için uygulanan güvenlik tedbirleri
- İşlemenin hukuki sebebi

Bununla beraber veri işlenen süreçlerin detaylarına ilişkin bilgiler, veri işlenen iş istasyonları, işlenen verinin niteliğine dair bilgi, verinin toplanma yöntemleri, verinin aktarım yöntemleri gibi ilave bilgiler ile hazırlanmış veri envanterinin niteliği arttırılabilir.

Veri envanteri süreç sahipleri tarafından beyan usulü olarak hazırlanabileceği gibi, veri keşif araçları ile de desteklenebilecektir.

Sicil başvurularında sicile açıklanacak bilgiler Kişisel Veri işleme Envanteri'ne dayalı olarak hazırlanmalıdır. Veri sorumluları sicilinde yer alan bilgilerle, envanterde yer alan bilgilerin tutarlı ve güncel olması banka tarafından yürütülen periyodik gözden geçirmeler ile sağlanır. Zira veri sorumluları, sicile sunulan ve sicilde yayımlanan bilgilerin eksiksiz, doğru, güncel ve hukuka uygun olmasından sorumludur.

1- Bankacılığa Özgü Veri Kategorileri

Veri envanterinde yer alan ve bankacılığa özgü olarak tanımlanan veri kategorilerinin başında finansal işlem kayıtları, borç/bakiye bilgileri, finansal istihbarat ve takip verileri, kredi risk skor bilgileri, finansal dolandırıcılık/ fraud verileri gibi veri kategorileri yer almaktadır

2- Kişi Grupları

Kişisel veri işleme envanterinde müşteri, başvuru sahibi, lehdar, kefil, garantör, hukuki halef, müşterek borçlu, risk grubunda yer alan kişiler için birinci derece yakınları, hissedar gibi bankacılık işlemleri kapsamında işlenen verilerin sahibi olan veri konusu kişi grupları olabileceği gibi; ziyaretçi, aday, personel, tedarikçi temsilcisi gibi kurumsal idare süreçlerinde işlenen verilerin sahibi olan veri konusu kişi grupları da yer alabilmektedir.

3- Alıcı Grupları

Veri envanterinde de ifade edilen bir diğer başlık olan alıcı grupları arasında; banka iştirakleri, iştirakleri ve grup firmaları, resmi kurumlar, Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamında tanımlanmış olan destek hizmeti kapsamındaki firmalar, destek hizmeti kapsamının dışındaki hizmet alınan taraflar, eğitim firmaları, bağımsız denetim firmaları, danışmanlık hizmeti alınan firmalar, avukatlık hizmeti alınan taraflar, varlık yönetim şirketleri, KKB / Risk merkezi gibi risk değerlendirme kurumları, muhabir bankalar, talimatlandırılmış hizmetler kapsamında finansal işlem kayıtlarının paylaşıldığı diğer finansal kuruluşlar, araştırma şirketleri gibi her bir veri işleme sürecine özgü olarak tanımlanabilecek alıcı ve alıcı grupları yer almaktadır.

4- Azami Süreler

Envanterde ifade edilen her bir veri kategorisi için süreç bazında azami saklama süresi belirlenmelidir. Bu süreler belirlenirken; mevzuatta öngörülen saklama süreleri, mevzuatta öngörülen bir sürenin bulunmaması halinde ise işlendikleri amaç için gerekli olan saklama süreleri;

a) İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
b) İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
c) İlgili veri kategorisinin işlenme amacına bağlı olarak veri

sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,

ç) İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,

d) Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,

e) Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,

f) Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi

dikkate alınarak belirlenir. Bu sürelerde referans alınabilecek düzenlemelerden bazıları;

- 15 yıl - İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği madde 7
- 10 yıl - 5510 sayılı Kanun madde 86
- 10 yıl - 5411 s. Bankacılık Kanunu
- 10 yıl - 6098 s. Türk Borçlar Kanunu
- 8 yıl - SPK Bilgi Suistimali veya Piyasa Dolandırıcılığı Suçları Hakkında
- Bildirim Yükümlülüğü Tebliği madde 10
- 3 yıl - Sermaye Piyasası Kurulu'nun VII-128.7 sayılı Sermaye Piyasasında
- Faaliyette Bulunanlar için Lisanslama ve Sicil Tutmaya ilişkin Esaslar
- Hakkında Tebliği madde 17/1
- 8 yıl - 5555 Suç Gelirlerinin Aklanmasının Önlenmesine Hakkında
- Kanun madde 8
- 8 yıl - Kimlik Paylaşım Sistemi Yönetmeliği madde 18

Bankalar, varlık durumu ve para hareketlerine dair her türlü araştırma ve raporlama verisini sağlayabilecek en temel ve tekil kuruluş olduğu için, saklama süreleri belirlenirken, teamülde resmi kurumların ihtiyaç duyduğu verilerin tarih aralığı da dikkate alınır. Bu durum bazen, bazı finansal verilerin kişiyi direkt olarak tarifleyen verilerden arındırılarak süresiz olarak

saklanmasını gerektirebilir. Böyle bir durumda ancak anonim hale getirilmiş kişisel veriler kişisel veri niteliğini haiz olmayacağından süresiz olarak saklanması mümkün olabilecektir.

Veri sorumluları sicilinde yer alan bilgilerden aşağıdakiler kamuya açıklanır:

a) Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişisinin adı, adresi ve alınmış olması halinde KEP adresi
b) Kişisel verilerin hangi amaçlarla işlenebileceği
c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri
ç) Kişisel verilerin aktarılabileceği alıcı ve alıcı grupları
d) Yabancı ülkelere aktarımı öngörülen kişisel veriler
e) Sicile kayıt tarihi ile kaydın sona erdiği tarih
f) Kişisel veri güvenliğine ilişkin alınan tedbirler
g) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

Veri sorumluları, sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, VERBİS üzerinden yedi gün içerisinde Kuruma bildirir.

C. Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi

1- Bankacılıkta Bilgilerin Saklanması

6102 sayılı Türk Ticaret Kanunu'nun 64, 65 ve 82'inci maddeleri ile 5411 sayılı Bankacılık Kanunu'nun 42'nci maddesi uyarınca, bankaların gerçekleştirdiği işlemlerle ilgili belgeleri 10 yıl süreyle saklama yükümlülüğü bulunmaktadır. Bunun yanı sıra bankalarca ürün ve hizmetlerin sunulması, bir sözleşme ilişkisini de doğurduğundan, saklama sürelerinin belirlenmesinde 6098 sayılı Türk Borçlar Kanunu'nun zamanaşımı sürelerini düzenleyen 146'ncı maddesinde yer alan her alacağın 10 yıllık zamanaşımına tabi olduğu hususu da göz önünde bulundurulur.

Diğer taraftan, Mevduat ve Katılım Fonunun Kabulüne, Çekilmesine ve Zamanaşımına Uğrayan Mevduat, Katılım Fonu, Emanet ve Alacaklara ilişkin Usul ve Esaslar Hakkında Yönetmelik ve düzenleyici kurumlarca (BDDK,

TMSF gibi) belirlenerek bankalara bildirilen bu hususlaki usul ve esaslar çerçevesinde, bankaların asgari olarak fona devir tarihine kadar saklama yükümlülüğü bulunmaktadır.

2- İşleme Amacının Ortadan Kalkması

Kişisel Verilerin Korunması Kanunu'nda, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gereğine yer verilmiştir. Kanunun "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7'nci maddesinde kişisel verilerin silinmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu da belirtilmiştir. Yönetmeliğin 7'nci maddesinin 1'inci fıkrasındaki düzenlemeden ise kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması ile Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkmasının kastedildiği anlaşılmaktadır.

Bankacılık açısından işleme amacı genel olarak, Bankacılık Kanunu'nun 4'üncü maddesinde belirlenen faaliyetlerin gerçekleştirilmesi ve mevzuat ile belirlenen yasal saklama sürelerine uyulması olarak özetlenebilecektir. Bununla birlikte, veri sorumlusu bankalar açısından insan kaynakları yönetimi, pazarlama, işyeri güvenliği gibi tüm veri sorumluları için geçerli olabilecek bankacılıktan kaynaklanmayan farklı işleme amaçlarının mevcut olabileceği de tabiidir. Bu hususlar her banka tarafından gerekli değerlendirmeler yapılarak oluşturulacak kişisel veri işleme envanteri ile saklama ve imha politikasında belirtilir.

Örnek olarak, aşağıdaki durumların tamamının birlikte gerçekleşmesi halinde, sürekli iş ilişkisi tesis edilen müşterilerle ilgili ilk işleme amacının ve kişisel verilerin saklanması suretiyle işlenmesi amacının ortadan kalktığı kabul edilmelidir.

- Müşterinin, hesaplarının kapatılarak, sürekli iş ilişkisine son verilmesi yönünde talebinin olması
- Sürekli iş ilişkisinin sona ermesini takiben, müşteri belgelerinin muhafazası konusunda yasal düzenlemelerden kaynaklanan saklama sürelerinin geçmiş olması
- Müşteri ile banka arasında devam eden herhangi bir hukuki ihtilafın bulunmaması
- Müşteri hesapları üzerinde, hesapların kapatılmasını engelleyecek herhangi bir haciz, rehin vb. kaydın bulunmaması

verilebilir.

İlgili kişilerin, Kanunun ilgili kişi haklarını düzenleyen 11'inci maddesinin birinci fıkrasının (e) bendi çerçevesinde kişisel verilerinin silinmesi veya yok edilmesine ilişkin talepte bulunması durumunda bankalar açısından derhal silme yükümlülüğü ortaya çıkmamaktadır. Detaylandırmak gerekirse, ilgili kişinin müşteri olması ve halihazırda devam eden ürün ve hizmet kullanımlarının bulunması (mevduat hesabı, kredi/kredi kartı borcunun devamı, fatura ödeme talimatı vb.) durumunda öncelikle ilgili kişiye bu kullanımların devam etmesi halinde işleme amacının devam ettiği ve mevzubahis amaçlar kapsamında işlenen kişisel verilerinin silinmesinin mümkün olmadığı yönünde yanıt verilebilecektir. Bu yönde talepte bulunan ilgili kişilere, ürün ve hizmet kullanımının sona erdirilmesi, karşılıklı borç ve alacakların sonlanması ile yukarıda belirtilen ilgili mevzuatta düzenlenen saklama sürelerinin geçmesinden sonraki ilk periyodik imhada taleplerinin yerine getirileceği yönünde yanıt verilmesi uygun olacaktır.

Kişisel verilerin korunmasına ilişkin mevzuatta ifade edilen işleme amacı kavramı, bankacılıkta ürün, hizmet, faaliyet bağlamında ve süreç bazında değerlendirilebilecektir. Bu durumda imha işleminin gerçekleştirilmesi için söz konusu ürün, hizmet, faaliyet veya sürecin sona ermesi ve bunlara ilişkin veri imha politikasında belirtilen saklama sürelerinin sona ermiş olması koşulunun sağlanması gözetilir. Mevzuatın lafzi bir yorumuyla ulaşılan sonuç bu şekilde olmakla birlikte bankaların faaliyetlerini kişisel verilerin korunmasına ilişkin bir düzenlemenin bulunmadığı, ağırlıkla sektöre özgü regülasyonların olduğu ve henüz dijitalleşmenin başlamadığı

bir faaliyet ortamında tasarlamış olmaları nedeniyle lafzi bir yorum ile ulaşılan amaç bazlı ayrıştırmanın bankaların veri mimarisine uygulanması uzun zaman ve yüksek maliyet gerektirmesinin yanı sıra verilerin bütünlüğü ve ulaşılabilirliği ile iş sürekliliğinin sağlanması yükümlülüğü açısından da riskler barındırmaktadır. Bu bakımdan kişisel verilerin imha sürecinin titizlikle yönetilmesi önem arz etmektedir.

Yukarıda yer verilen hususlar doğrultusunda her bir banka kendi kaynaklarını, veri ve süreç mimarisini göz önünde bulundurarak kısa, orta ve uzun vadeli imha hedeflerini belirlemelidir. Kademeli olarak erişilecek amaç bazlı imha yapısı (bir verinin imhasının, ilişkili diğer verilerinin tutarlılığını ve hesap verilebilirliğini bozmaksızın gerçekleştirilebilmesi) tesis edilinceye kadar işleme amacı sona eren kişisel verilerin imhasında bankalar kendi sistemlerine uygun teknik ve idari tedbirleri almalıdırlar.

Bankacılık sektöründe bilgi sistemlerinin girift yapısı, birçok bankacılık ürününün oluşturduğu verideki bir değişikliğin diğer ürünlerin verilerine sirayet etmesine, bir ürünün verilerinin ortadan kaldırılmasının diğer ürünlerin verilerinin de bir kısmının karanlıkta kalmasına, kopuk bir muhasebe hareketi silsilesi izlenmesine ve anlaşılmasının güçleşmesine neden olmaktadır. Örneğin, bir gerçek kişiye ait veri yığınının her bir tekil elemanının (örneğin, o kişinin kredisinin belirli bir tarihteki tahsil hareketi) aslında diğer tekil elemanların muhasebe ve bilgi işlem bağlamında tutarlı ve bütünsel bir şekilde izlenmesine olanak vermesi için de tutulması ve saklanması gerekebilmektedir. Bu kapsamda, bir gerçek kişinin herhangi bir tekil verisi için işleme amaçları arasında "veri bütünlüğünün korunması", "müşteri bilgilerinin tutarlılığının sağlanması" gibi amaçlar da bulunmaktadır. Bu amaçların Kanun'un 5'inci maddesinin ikinci fıkrasının (ç) bendindeki veri sorumlusunun özellikle hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması (örneğin BDDK düzenlemeleri) ve f bendindeki ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması kapsamında ele alınabileceği düşünülmektedir.

3- İmha Yöntemleri

Yönetmeliğin 7'nci maddesinin 5'inci fıkrasında veri sorumlularına imha için silme, yok etme veya anonim hale getirme yöntemlerinden birini seçme imkanı tanınmıştır. Yönetmelik kapsamında kişisel verilerin; silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi,yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi, anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi olarak tanımlanmıştır. Bu yöntemlerin teknik açıdan değerlendirilmesine aşağıdaki tabloda yer verilmişti

İmha Yöntemi	Teknik Açıklaması	Uygulanabilecek Teknikler	Avantajlar	Dezavantajlar	Muhtemel Riskler	Örnek Uygulanabilecek Bankacılık Uygulamaları
Silinme	Teknik olarak veriye ilgili kullanıcıların erişiminin kaldırılması kanundaki silme yönteminin gereksinimlerini karşılamaktadır.	Veriyi bankacılık uygulamalarında ilgili kullanıcıların erişimine ve tekrar kullanımına kapama		Mevcut bankacılık uygulamalarında yüksek miktarda değişiklik gerekecektir. Veriler, veri sistemlerinde yer kaplamaya devam edecektir.	Yetkilendirme noktalarında eksikler olabileceğinden orta yüksek risk içermektedir.	Tüm bankacılık alanlarında uygulanabilir. Örneğin "Silinecek verilerin oluşturulacak profilde yer alan sınırlı kullanıcılar dışında genel müdürlük ve şube çalışanlarına kapatılması" gibi. Verinin hala sistemlerde yer kapladığı unutulmamalı buna göre kapasite planlaması yapılmalıdır. Silinen veriye nasıl ve hangi şartlar altında erişim sağlanacağı belirlenmelidir.
		Veriyi dosya veritabanı seviyesinde ilgili bankacılık uygulamalarının erişimine kapama		Dosya sunucusu veritabanı üzerinde operasyonlar gerektirmektedir. Veriler, veri sistemlerinde yer kaplamaya devam edecektir.		
		Veri izole ve korunaklı bir ortama (karantina bölgesi) taşınır.	Veri izole bir ortama alındığı için ilgili kullanıcıların erişimine ve tekrar kullanımına kapalı olacaktır.	Veriler, veri sistemlerinde yer kaplamaya devam edecektir.	Düşük de olsa veri bütünlüğünü bozma riski bulunmaktadır.	

İmha Yöntemi	Teknik Açıklaması	Uygulanabilecek Teknikler	Avantajlar	Dezavantajlar	Muhtemel Riskler	Örnek Uygulanabilecek Bankacılık Uygulamaları
Yok Etme	Teknik olarak verinin bulunduğu ortamdan geri getirilemez biçimde imha edilmesini ifade eder.	Veri dosyaları kayıtları geri döndürülemeyecek şekilde (PURGE-NOLOGGING gibi yöntemlerle) yok edilir.	Verinin hiçbir şekilde geri döndürülemez olması.		Düşük de olsa veri bütünlüğünü bozma riski bulunmaktadır.	Tüm bankacılık alanlarında uygulanabilir. Örneğin "Bir müşteriye ait fiziksel belgelerin kağıt imha makinasından geçirilmek suretiyle imha edilmesi" gibi.

İmha Yöntemi	Teknik Açıklaması	Uygulanabilecek Teknikler	Avantajlar	Dezavantajlar	Muhtemel Riskler	Örnek Uygulanabilecek Bankacılık Uygulamaları
Anonim Hale Getirme	Verinin bulunduğu ortamda ilgili kişi ile hiçbir şekilde ilişkilendirilemeyecek hale getirilmesini ifade eder.	Veri dosyaları ve kayıtları üzerinde anonimleştirme yapılır. Uygulanabilecek birçok teknik bulunmaktadır. Verilerin anonim hale getirilmesinde kayıt ortamı ve ilgili faaliyet alanı göz önünde bulundurularak uygun tekniğin belirlenmesi gerekmektedir.	Kayıtlarda sadece belirli alanların imhası için uygulanabilir.	Tüm uygulamalar ve entegrasyonları bazında ve raporlamalar kapsamında çok detaylı analiz gerektireceğinden uzun soluklu ve maliyetleri yüksek bir imha yöntemi olacaktır.	Anahtar veri konumundaki kişisel veri alanlarından dolayı veri bütünlüğünü bozmamak için çok dikkatli uygulanmalıdır; risk olasılığı ve derecesi yüksek bir yöntemdir.	Muhasebe hareketleri gibi eski tarihli finansal verilerde sadece belirli kişisel veri alanlarının anonimleştirilmesi için kullanılabilir.

D. Veri Güvenliği

Veri sorumlusu sıfatını haiz bankaların 6698 sayılı Kanun'un 12'nci maddesi uyarınca veri güvenliğine ilişkin yükümlülükleri bulunmaktadır. Bankaların aşağıda detayları sunulan kendi mevzuatı kapsamında tabi olduğu yükümlülükler de 6698 sayılı Kanundan kaynaklanan yükümlülüklerine uyulmasında katkı sunmaktadır.

1- Bankaların Yasal Mevzuattan Kaynaklanan Yükümlülükleri

Bankalar, bankacılık işlemlerinin güvenliğinin sağlanması için 5411 sayılı Bankacılık Kanunu, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, Sermaye Piyasası mevzuatı gibi çeşitli düzenlemelere tabi kılınmıştır.

1.1. Bankacılık Kanunu

5411 sayılı Bankacılık Kanunu'nun "Sırların Saklanması" konu başlıklı 73'üncü maddesi, banka mensupları için "görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar" hükmünü içermektedir.

1.2. Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik

BDDK tarafından yayımlanan bu Yönetmelik hükümlerine ilişkin olarak ayrıntılı açıklamalara aşağıda "Denetim" başlığında altında yer verilmektedir.

1.3. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

Bu yönetmelik, faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis

edilmesi gereken bilgi sistemleri kontrollerini düzenlemiş olup, bu haliyle 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bağlı mevzuatta kişisel veriler için öngörülen teknik ve idari tedbirleri kapsamaktadır.

KVKK ile paralel kaleme alınmış maddelerden biri olarak açık bankacılık[54] faaliyetleri için veri paylaşımının söz konusu olacağı noktada müşterinin talebi olmaksızın paylaşımın yapılamayacağı belirtilerek Müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesi verilecek hizmet için bir ön şart haline getirilemeyeceği düzenlenmiştir.[55]

Kişisel Verileri Koruma Kurumu tarafından benzer içerikte ilişkili yayın Kişisel Veri Güvenliği Rehberi (Teknik ve idari Tedbirler) olarak görünmektedir. Bu belgede yer alan Teknik Tedbirler başlığındaki birçok madde Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik 'le örtüşmektedir. Konuya ilişkin yapılan eşleştirme "Bilgi Güvenliğine ilişkin Teknik ve idari Önlemler" başlığında yer almaktadır.

1.4. Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik

Bu yönetmelik, banka sırrı ve müşteri sırrı niteliğindeki bilgilerin paylaşım ve aktarımlarına ilişkin kapsam, şekil, usul ve esasları belirleyerek, bilgi paylaşımındaki ilkeleri ve yükümlülükleri belirleyerek, alınması gereken idari tedbirlere yer vermiştir.

1.5. Bilgi Güvenliğine İlişkin Teknik ve İdari Önlemler

Bankacılık sektörü, Kişisel Verilerin Korunması Kanunu ve diğer kanunlara ek olarak; Bankacılık Kanunu ile Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından yayınlanan ikincil mevzuata tabidir. Bu çerçevede, bankalar, bilgi sistemlerinin işlerliğini ve güvenliğini sağlamak için gerekli önlemleri

[54] Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, FTP gibi yöntemlerle bankanın sunduğu bir takım finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanallarını" ifade etmektedir.

[55] Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Madde 10

almakla yükümlüdür. Bankacılık sektörüne özgü düzenlemeler, kişisel veriler dahil olmak üzere tüm müşteri ve banka bilgilerinin güvenliğinin sağlanmasını amaçlamaktadır. Ayrıca, Bankacılık Kanunu'nda yer alan gizlilik yükümlülükleri de banka bünyesinde sıkı sıkıya uygulanmakta olup, bu durum bilgi güvenliği ve kişisel verilerin korunması açısından hayati öneme sahiptir. Kritik altyapı, işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran sistemlerdir. Bankacılık alanında faaliyet gösteren veri sorumlularının da bu kapsamda değerlendirileceği dikkate alındığında Bankacılık sektörünün veri güvenliği açısından uyum sağlaması gereken bazı mevzuat, düzenleme ve standartlar;

- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik,
- "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı,
- Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (Payment Card Industry -PCI- Data Security Standard -DSS-),

olup, bu düzenlemelerin birbirleri ile örtüşen yönleri bulunmaktadır.

Kurul tarafından yayınlanan Kişisel Veri Güvenliği Rehberi'nde yer alan Teknik Tedbirler özet tablosunun, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ile kıyaslanmasında karşılık gelen maddeleri aşağıdaki tabloda gösterilmiştir.

TEKNİK TEDBİRLER	Yetki Matrisi	Kimlik ve Erişim Yönetimi Md.11
	Yetki Kontrol	Kimlik ve Erişim Yönetimi Md.11
	Erişim Logları	Kimlik ve Erişim Yönetimi Md.11 İz Kayıtlarının Oluşturulması ve Takibi Md.13
	Kullanıcı Hesap Yönetimi	Kimlik ve Erişim Yönetimi Md.11
	Ağ Güvenliği	Ağ Güvenliği Md.14
	Uygulama Güvenliği	Güvenlik Konfigürasyonu Yönetimi Md.15, Güvenlik Açıkları ve Yama Yönetimi Md.16,
	Şifreleme	Veri Gizliliği Md.9, Erişilebilirlik Yönetimi ve Yedekleme Md.21 Kimlik Doğrulama ve İşlem Güvenliği, Md.34,
	Sızma Testi	Siber Olay Yönetimi, Sızma Testi ve Siber İstihbarat Paylaşımı Md.18
	Saldırı Tespit ve Önleme Sistemleri	Ağ Güvenliği Md.14, Siber Olay Yönetimi, Sızma Testi ve Siber İstihbarat Paylaşımı Md.18
	Log Kayıtları	Kimlik ve Erişim Yönetimi Md.11, İz Kayıtlarının Oluşturulması ve Takibi Md.13
	Veri Maskeleme	Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik Md.6
	Veri Kaybı Önleme Yazılımları	Güvenlik Konfigürasyonu Yönetimi Md.15, Güvenlik Açıkları ve Yama Yönetimi Md.16
	Yedekleme	Erişilebilirlik Yönetimi ve Yedekleme Md.21
	Güvenlik Duvarları	Ağ Güvenliği Md.14
	Güncel Anti-Virüs Sistemleri	Güvenlik Konfigürasyonu Yönetimi Md.15, Güvenlik Açıkları ve Yama Yönetimi Md.16
	Silme, Yok Etme veya Anonim Hale Getirme	Bankacılık Kanunu Md.42
	Anahtar Yönetimi	Veri Gizliliği Md.9, Kimlik Doğrulama ve İşlem Güvenliği Md.34

İdari tedbirler başlığı beklenen faaliyet konusu KVKK'ya ilişkin beklenen aktiviteler ile örtüşmesine rağmen faaliyet içeriği açısından farklılaşmaktadır.

Kişisel Veri Güvenliği Rehberi idari tedbirler bölümü ile Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'i (Yönetmelik) karşılaştırdığımızda bankacılık sektöründe karşılık gelen konuları aşağıdaki gibi özetleyebiliriz.

- Kişisel Veri Güvenliği Rehberi Mevcut Risk ve Tehditlerin Belirlenmesi

Bankalar, bilgi varlıklarının[56] güvenlik gereksinimlerine uygun kontroller tesis etmek için bu varlıkları sınıflandırarak detaylı bir varlık envanteri hazırlar. Bilgi varlıklarının bir parçası olan veriler için kişisel veri olup olmadığı kontrol edilir. Verilerin güvenlik sınıfı asgari olarak bu verilerin gizlilik derecesi, bütünlük gereksinimi, erişilebilirlik gereksinimi ve hassas veri, kişisel veri ya da sır kapsamındaki veri olup olmadığı gibi kriterler göz önünde bulundurularak belirlenir. **(Bilgi varlıkları envanteri ve sınıflandırılması Madde 6)**

Bankalar, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir BS risk yönetim süreci tesis eder. Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek bankanın BS risk envanteri oluşturulur. BS risk envanteri kapsamında riskler takip edilerek yönetim kuruluna ve üst düzey yönetime yılda en az bir defa raporlanır. (Bilgi sistemleri risk yönetim süreci Madde 7)

- Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Yönetmeliğin 19.maddesi (Bilgi Güvenliği Farkındalığını Artırma) gereğince;

[56] Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Madde 3 Tanımlar Bilgi varlığı: Bankacılık faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri gibi Banka için değeri olan varlığı,

Banka genelinde bilgi güvenliği farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturması sağlanır. Bu eğitim programı Bilgi Güvenliği Komitesi tarafından onaylanır ve programın içeriği yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilir ve güncellenir.

Bu eğitim programının haricinde kurum içi bültenler hazırlar, varsa banka iç portalında bilgi güvenliği ile ilgili bir bölüm oluşturur, çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma mesajları gönderir, çalışanlara yönelik düzenli olarak bilgi güvenliği farkındalığını ölçecek anketler yapar.

Üst yönetim de dâhil olmak üzere banka çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmaların yapılması sağlanır. (Bilgi güvenliği organizasyonu, roller ve sorumluluklar Madde 8)

- Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

Bilgi güvenliği yönetim sisteminin banka genelinde nasıl uygulanacağı bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlenir. Bankanın bilgi güvenliği politikası yönetim kurulu tarafından onaylanır ve banka genelinde çalışanlara ulaştırılması sağlanır. Bu kapsamda bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenir. (Bilgi güvenliği organizasyonu, roller ve sorumluluklar Madde 8/2)

Yönetmelik gereğince bankanın Bilgi Güvenliği Politikası ve bu çerçevedeki diğer ilgili prosedürler de yer alan Yönetmelik maddelerine aşağıda yer verilmiştir.

- Bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanları (Madde 5)
- Bilgi güvenliği yönetim sisteminin banka genelinde nasıl uygulanacağıbilgi güvenliği politikası, prosedürleri ve süreç

dokümanları (Madde 8)
- Siber olay yönetimi, çözüm prosedürü ve müdahale planları (Madde18)
- Değişiklik yönetimi süreçleri kullanıcı dokümanları ve prosedürleri (Madde 24)
- Erişilebilirlik yönetimi dokümanları ve yedekleme prosedürü (Madde 27)
- Bilgi sistemleri sürekliliğinin sağlanması kapsamında kurtarma ve geri dönüş prosedürleri (Madde 28)
- Dış hizmet alımı sürecinin yönetimi için gerekli prosedürler (Madde 29)

Yönetmeliğin 29'uncu maddesi (Dış Hizmet Alımı Sürecinin Yönetimi) gereğince; Banka üst yönetimi, dış hizmet[57] olarak alınacak hizmetlerin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayan yeterli bir gözetim mekanizması tesis edilmesini sağlar.

Bu kapsamda dış hizmetin doğuracağı risklerin belirlenmesi, hizmet alımına ilişkin koşul, kapsam ve tanımlar yazılı sözleşmeye bağlanır. Sözleşme dış hizmetlerin erişilebilirliğinin, performansının, kalitesinin, taahhüt edilen hizmet seviyelerine uyulup uyulmadığının, bu hizmetler kapsamında gerçekleşen güvenlik ihlali olaylarının, dış hizmet sağlayıcının gizlilik, bütünlük ve erişilebilirlik ile ilgili güvenlik kontrollerinin, operasyonel ve finansal durumunun yükümlülüklerini yerine getirmeye uygun olup olmadığının ve sözleşme şartlarına uygunluğunun düzenli aralıklarla takip edilmesi sağlanır.

- Kişisel Verilerin Mümkün Olduğunca Azaltılması

Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmeliğin 5'inci maddesi kapsamında yapılacak paylaşımların ölçülü olabilmesi için;

[57] Dış hizmet: 5/11/2011 tarihli ve 28106 sayılı Resmi Gazete'de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri de dâhil olmak üzere bankaların bilgi sistemlerine ilişkin dışarıdan temin ettikleri, bankacılık verilerinin gizliliği, bütünlüğü ve erişilebilirliği ile bankacılık hizmetlerinin sürekliliğini etkileme potansiyeli olan, bankacılık verilerine erişimi bulunan ya da bu verilerin paylaşıldığı hizmet alımlarını,

- Belirtilen hangi amaçlarla ilişkili ise, paylaşımların yalnızca söz konusu amaçların gerektirdiği kadar veriyi içermesi,
- Paylaşımların içerdiği veri ya da veri setlerinin tamamının belirtilen amaçların gerçekleştirilmesi için gerekli olduğunun gösterilebilir olması,
- Paylaşılacak veriler toplulaştırıldığında, kimliksizleştirildiğinde ya da anonim hale getirildiğinde söz konusu amaçlar yine de gerçekleştirilebiliyor ise bu yöntemlerin uygulanması,
- Paylaşım yapılacak tarafların ve paylaşım metotlarının mümkün olan en az veri kopyası oluşturacak şekilde kurgulanması unsurların asgari olarak yerine getirilmesi zorunlu kılınmıştır.

2- Denetim

5411 sayılı Bankacılık Kanunu'nun 29'uncu maddesi "Bankalar, maruz kaldıkları risklerin izlenmesi, kontrolünün sağlanması, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tâbi ortaklıklarını kapsayan yeterli ve etkin bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlüdürler" ifadesini içermektedir. Uygulama detayları Bankaların iç Sistemleri ve içsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik ile düzenlenen bu hususun bankalara getirdiği yükümlülüklerin uygulanması, denetim sistemi kurma yükümlülüğü bulunmayan çok sayıda başka sektörü de düzenleme misyonu bulunan 6698 sayılı Kanun'un 12'nci maddesinin 3'üncü fıkrası çerçevesinde denetim yükümlülüğünü her yönüyle kapsamaktadır. Kişisel Verileri Koruma Kurumunun yayımlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve idari Tedbirler)'nde de denetim hususunda belirtildiği üzere veri sorumlusu, kişisel veri içeren sistem üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir.

Bankaların iç denetim birimleri, bağlı oldukları ve denetim yükümlülüğünü düzenleyen mevzuat uyarınca 6698 sayılı Kanun'da belirtilen denetim yükümlülüklerini karşılamaktadırlar.

KVKK'nın 12'nci maddesinin 3'üncü fıkrası hükmü çerçevesinde yapılan tüm bilgi teknolojileri denetimlerinde; BDDK'nın Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ve BDDK tarafından yayınlanan Bilgi Sistemlerine ilişkin Sızma Testleri Genelgesi uyarınca alınması gerekli teknik ve idari tedbirlerin kontrolü sağlanır.

Ayrıca bankalar, 6698 sayılı Kanun'un 12'nci maddesi hükmüne istinaden aldıkları güvenlik önlemlerinin uygulanmasında aynı zamanda Bankaların iç Sistemleri ve içsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin içerisinde düzenlenen iletişim kanallarının tesisinde, Bankacılık Kanunu'nun 73'üncü maddesine aykırılık teşkil edilmemesi hususuna da özen göstermektedir.

Bankalar 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ve Banka Kartları ve Kredi Kartları Hakkında Yönetmelik kapsamında kart çıkarılması, kullanım ve kartlı ödemeler sisteminde yer alan kuruluş olarak faaliyet göstermektedir.

Bu kanun ve yönetmelik gereği bu hizmetleri veren bankalar; Veri işleme, kaydetme veya iletişiminde asgari seviyede uluslararası standart olan Ödeme Kartı Endüstrisi Veri Güvenliği Standardının (Payment Card Industry -PCI- Data Security Standard -DSS-) hükümlerini dikkate alırlar.

Bankalar bilgi güvenliği süreçlerini etkin yürütmek ve sürdürebilmek için uluslararası standart olan ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (BGYS)'nin standardının gereklerini yerine getirecek şekilde kaynakların tahsis ederek, kurulması ve işletilmesini sağlarlar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı bankalarda yer alan risklerin daha somut bir şekilde ölçülebilmesini ve değerlendirmesini sağlayarak bilgi güvenliği konusunda daha etkin önemlerin alınmasını sağlayan bir standarttır.

ISO/IEC 27001 ve PCI DSS standartları çerçevesi, kişisel verilerin güvenliğiyle sınırlı kalmamak üzere sahip olunan tüm verilerin güvenliğine yönelik bir

güvenlik seviyesi ve metodolojisi içermektedir. Söz konusu standartlar çerçevesine uyumlu olduğu konuyla ilgili periyodik denetim ve raporlarla tespit edilmiş her banka, 6698 sayılı Kanunun gerektirdiği veri güvenliği yükümlülüğünü sağlamak adına alınacak tedbirlere destekleyici nitelikte tedbirler almış olacaktır.

ISO/IEC 27701 Kişisel Veri Yönetim Sistemi standardı kişisel veri işleyen veri sorumluları ve veri işleyenlerin sorumluluklarına yönelik rehberlik eden, kişisel veri yönetim sisteminin gereksinimlerini ortaya koyarak hesap verilebilir bir sistem geliştirmeyi sağlayan bir standarttır.

E. İlgili Kişinin Hakları ve Şikâyetlerin Yönetilmesi

Anayasanın 20'nci maddesinde; *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* şeklinde hüküm bulunmaktadır.

Dolayısıyla, kişisel verilerin korunmasını isteme hakkı, esasında Anayasa'da da güvence altına alınmış bir haktır. Dayanağını Anayasa'dan alan bu hakkın kullanılmasına ilişkin açıklamalara aşağıda yer verilmektedir.

1- Veri Sorumlusu Temsilcisi

Veri sorumlusu temsilcisi; Türkiye'de yerleşik olmayan veri sorumlularını asgari temsile yetkili Türkiye'de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi ifade eder.

Veri sorumlusu temsilcisinin, 30 Aralık 2017 tarihli ve 30286 sayılı Resmî Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin

("Yönetmelik") 11'inci maddesinin (c) bendi uyarınca "Kişisel Verileri Koruma Kurulu (Kurul) tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanun'un 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme" ve (ç) bendi uyarınca "Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanun'un 13'üncü maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme" yükümlülükleri bulunmaktadır.

2- Başvuru ve Şikayetlerin Alınması ve Yanıtlanması

Kanun'un 3'üncü maddesinde ilgili kişi; "kişisel verisi işlenen gerçek kişi" olarak tanımlanmıştır. Bu kapsamda tüzel kişiler ilgili kişi sıfatıyla veri sorumlusuna başvuruda bulunamaz.

Kanun, ilgili kişilerin Kanun'un uygulanmasına ilişkin taleplerini iletebilmeleri ve kişisel verilerine ilişkin haklarını korumaları için birtakım hak arama yöntemleri getirmektedir. Böylelikle ilgili kişiler kişisel verilerinin korunmasına ilişkin haklarını kullanmak adına doğrudan yargı yoluna başvurmanın yanı sıra Kanun'un 11'inci maddesindeki haklarını kullanabileceklerdir. Kanun'da başvuru ve şikâyetlerle ilgili usul ve esaslar 13, 14 ve 15'inci maddelerde düzenlenmiştir.

2.1. Veri Sorumlusuna Başvuru

Veri sorumlusuna başvuru usul ve esasları Kanun'da ve 10 Mart 2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkında Tebliğ'de ("Tebliğ") düzenlenmektedir. Kanun'un 11'inci maddesine göre ilgili kişilerin veri sorumlusuna başvurusu için kademeli bir başvuru usulü öngörülmüştür. İlgili kişinin sahip olduğu hakları kullanabilmeleri için öncelikle veri sorumlusuna başvurmaları zorunludur. Bu yol tüketilmeden Kurula şikayet yoluna gidilmesi mümkün değildir. Tebliğ'in 5'nci maddesi başvuruda yer alması gereken unsurları düzenlemektedir.

Buna göre başvuruda bulunması gereken zorunlu unsurlar aşağıdaki gibidir:

- Ad-Soyad
- TC Kimlik No (başvuran Türk vatandaşı ise)
- Tebligata esas ikametgah veya işyeri adresi
- Başvuru yazılı ise imza
- Uyruk, Pasaport No/Varsa Kimlik No (başvuran Türk vatandaşı değilse)
- Varsa bildirime esas e-posta adresi, telefon, faks no
- Talep Konusu

2.1.1. Şekil ve Usul

Veri sorumlusuna yapılacak başvuruların şekli konusunda Kanun'da iki temel hüküm bulunmaktadır. Bunlardan ilki yazılı başvuru olup, genel hükümler gereği ıslak imza içeren belge ile yapılan başvurudur. Buna ek olarak elektronik ortamda da başvuru yapılabilmektedir. Yazılı başvuru haricindeki diğer yöntemler konusunda ise Kurul yetkilendirilmiş olup, Kurul buna istinaden Tebliğ'in 5'inci maddesinde veri sorumlusuna yapılacak başvuruların yöntemini belirlemiştir. Buna göre; ilgili kişi veri sorumlusuna Türkçe olarak;

- Yazılı,
- KEP adresi,
- Mobil imza,
- Güvenli Elektronik imza,
- E-posta (ilgili kişi tarafından veri sorumlusuna daha önce bildirilen,veri sorumlusunun sisteminde kayıtlı bulunan dolayısıyla kimlik doğrulamasının yapılabildiği elektronik posta adresi),
- Başvuru Yazılımı/Uygulaması (veri sorumlusunun başvuru amacına yönelik geliştirmiş olabileceği bir yazılım ya da uygulama)

yöntemlerinden birini kullanarak başvurabilecektir.

Veri sorumlusu başvuruda yer alan talepleri talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandıracak, ancak

işlemin ayrıca bir maliyeti gerektirmesi halinde Kurulca belirlenen tarifedeki ücret alınabilecektir.

Kanun'un 13'üncü maddesi gereğince ilgili kişinin talebi ücretsiz olarak sonuçlandırılır. Tebliğ'in 6'ncı ve 7'nci maddesi uyarınca;

- Yazılı olarak verilecek cevaplarda, 10 sayfaya kadar ücret alınmaz iken 10 sayfanın üzerindeki her sayfa için 1 Türk lirası işlem ücreti alınabilir,
- Cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez,
- Başvurunun, veri sorumlusunun hatasından kaynaklanması halinde alınan ücret ise ilgiliye iade edilir.

Bu düzenlemeler uyarınca, Bankanın en yakın şubesine ilgili kişinin kimliğini tevsik edici belgeler ve talebini içeren yazılı dilekçe ile bizzat elden veya Kurulca belirlenen diğer yöntemleri kullanmak suretiyle alınmış olan başvurular, zorunlu olarak bulunması gereken yasal şartları içermesi halinde en kısa sürede ve en geç otuz gün içinde sonuçlandırılacaktır.

30 günlük süre, yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih itibariyle, diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih itibariyle başlayacaktır.

Bankanın ilgili iş birimlerinde yapılacak araştırma sonucunda ilgili kişinin başvurudaki talepleri kabul edilebileceği gibi gerekçesi açıklanmak suretiyle ret de edilebilir.

Örneğin, ilgili kişiden kişisel verilerinin imhası hakkında alınmış bir başvuruda, veri işlemenin hukuka uygunluk nedenlerinin devam edip etmediği ve hukuka uygunluk nedenlerinin ortadan kalkmış olması halinde, verilerin yasal saklama sürelerinin devam edip etmediği kontrol edilir. Veri işlemenin hukuka uygunluk nedenlerinin devam etmesi halinde ya da hukuka uygunluk nedenlerinin ortadan kalkmış olması ile birlikte yasal saklama sürelerinin devam ediyor olması halinde, talep olumsuz olarak yanıtlanır.

Başvuruda zorunlu yasal şartların bulunmadığının tespit edilmesi halinde ise başvuru reddedilir ve ilgili kişiye ret gerekçesi ile bildirilir.

Tebliğ'in 6'ncı maddesi göre, veri sorumlusunun cevabında bulunması gereken asgari unsurlar aşağıdaki gibidir:

Veri sorumlusu veya temsilcisine ait bilgiler,

- Başvuru sahibinin adı ve soyadı, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası,
- Talep konusu,
- Veri sorumlusunun başvuruya ilişkin açıklamalarıdır.

Tebliğ'in 6'ncı maddesine göre veri sorumlusu cevabını mutlaka ya yazılı ya da elektronik ortamda göndermelidir.

2.2. Kurula Şikayet

İlgili kişinin veri sorumlusuna başvurusu sonucunda veri sorumlusu tarafından;

- Başvurunun reddedilmesi,
- İlgili kişi tarafından verilen cevabın yetersiz bulunması,
- Süresinde başvuruya cevap verilmemesi

halinde ilgili kişi Kurula şikayette bulunabilir. Kanun'un 14'üncü maddesi, Kurul'a şikayet için altmış günlük bir süre öngörmüştür. Bu altmış günlük sürenin başvuruya cevap alınamadığı, başvuruya verilen cevabın yetersiz görüldüğü veya 30 günlük sürenin sonrasında ilgili kişi başvurusuna cevap verildiği durumlarda hangi andan itibaren başlayacağı tartışma konusu olmuştur. Kurulun 24.01.2019 tarihli ve 2019/9 sayılı kararı ile;

- İlgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyette bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu

tarihten itibaren 60 günlük süresinin bulunmadığı,

- İlgili kişi tarafından yapılan başvuruya veri sorumlusunca bir cevap verilmediği durumda ise ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği,
- İlgili kişi tarafından yapılan başvuruya veri sorumlusunca Kanun'da tanınan 30 günlük süre sonrasında bir cevap verilmesi halinde ilgili kişinin, Kanun'da veri sorumlusuna tanınan 30 günlük süre sonrasında verilecek cevabı beklemekle yükümlü olmadığı ve veri sorumlusuna tanınan sürenin dolması ile birlikte Kurula şikâyette bulunabileceği göz önüne alınarak, ilgili kişinin veri sorumlusunun kendisine cevap verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği

belirtilmiştir.

2.2.1. Kimlik Tespiti/Doğrulama

Bir kişinin iddia ettiği kişi olup olmadığının tespit edilmesine kimlik tespiti/doğrulama denilmektedir. Kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi ve veri güvenliğinin sağlanması gereği olarak, alınan bir başvuruda ancak kimlik tespitinin yapılabiliyor olması halinde başvurunun kabul edilebilmesi, alınması gereken makul bir önlem olarak kabul edilir. Kurul'un 06.05.2021 tarihli ve 2021/470 sayılı kararına konu olayda ilgili kişi veri sorumlusunun sisteminde tanımlı olmayan bir e-posta adresinden başvuru yaparak belirli bir hesabın hareketlerine erişmek istemiştir. Veri sorumlusu ilgili hesap hareketlerini şifreleme yöntemi kullanarak paylaşmış ve gönderilen e-postadaki telefon numarasının aranması ile şifre anahtarının paylaşılacağını belirtmiştir. Kurul bu durumda, ilgili kişilerin kişisel verilerinin yetkisiz üçüncü kişilerin eline geçmemesi için veri sorumlusu tarafından kullanılan yöntemi Kanun'a uygun bulmuştur. Bu bakımdan, kişisel verileri ile ilgili bilgi talep eden ilgili kişinin kimlik tespitinin yapılabiliyor olması, başvurusunun kabul edilebilir olabilmesi için zorunlu olup, ilgili kişinin başvurusu ile birlikte kimliğini tevsik edici belgeleri de ulaştırması gerekmektedir. Aksi takdirde üçüncü bir kişiye, bir başkası hakkında kişisel veri niteliğinde bilgilerin iletilmesi ile veri güvenliğinin ihlaline sebebiyet verilmesi söz konusu olacaktır.

Ayrıca, Bankacılık Kanunu'nun 73'üncü maddesi uyarınca da müşteri sırrının ihlali niteliğinde değerlendirilebilecek bu durumda bankalara Kanun'un 159'uncu maddesi uyarınca cezai yükümlülük öngörülmektedir.

Örneğin, Bankaya daha önce bildirilmemiş, dolayısıyla sistemde kayıtlı bulunmayan bir elektronik posta ile yapılmış bir başvuruda, başvurucunun kimlik tespitinin yapılması mümkün olmadığından, başvurunun zorunlu olarak bulunması gereken yasal şartları içermediği gerekçesi ile reddedilir.

Kimlik teyidinin yapılamadığı mecralardan yapılacak başvurularda, başvurunun kabul edilmesi bankanın ihtiyarında olup, ilgili kişiler kimlik tespiti yapılabilen güvenli başvuru kanallarına yönlendirilebilecektir.

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

ARALIK 2024

Nasuh Akar Mah. 1407. Sokak No: 4 06520
Balgat - Çankaya / ANKARA
Telefon: +90 312 216 50 00
Web: www.kvkk.gov.tr