



BİLGE BANK A.Ş.

KASIM 2023

BİLGE BANK A.Ş.
AVRUPA BİRLİĞİ GENEL VERİ KORUMA POLİTİKASI
BİLGİ FORMU

Doküman Adı: Bilge Bank A.Ş. Avrupa Birliği Genel Veri Koruma Politikası

Hedef Kitle: Bilge Bank A.Ş. tarafından kişisel verileri işlenen Bilge Bank A.Ş.'nin çalışanları dışındaki veri sahipleri

Hazırlayan: Bilge Bank A.Ş. Kişisel Verileri Koordinasyon Birimi

Versiyon: 1.0

Yürürlük Tarihi: 17.09.2023

İlk yayım tarihi: Ocak 2023

İşbu Bilge Bank A.Ş. Avrupa Birliği Genel Veri Koruma Politikası'nın hazırlanmış olduğu Türkçe dilindeki hali ile herhangi bir dilde çeviri hali arasında uyumsuzluk çıkması durumunda Türkçe metin esas alınmalıdır.

© Bilge Bank A.Ş., 2023

İşbu Bilge Bank A.Ş. Avrupa Birliği Genel Veri Koruma Politikası Bilge Bank A.Ş.'nin yazılı izni olmaksızın çoğaltılıp dağıtılamaz.

BİLGE BANK A.Ş.

BÖLÜM 1. AMAÇ, KAPSAM VE TANIMLAR	5
AMAÇ	5
KAPSAM	7
BÖLÜM 2. PRENSİPLER	15
2.1. Kişisel Verilerin İşlenmesine İlişkin İlkeler (Madde 5)	15
2.2. İşlemenin Yasallığı (Madde 6)	18
2.3. Rıza Koşulları (Madde 7)	19
2.4. Bilgi Toplumu Hizmetlerine İlişkin Olarak Çocuğun Rızasına İlişkin Koşullar (Madde 8)	19
2.5. Özel Nitelikli Kişisel Verilerin İşlenmesi (Madde 9)	20
2.6. Ceza Mahkûmiyeti ve Suça İlişkin Kişisel Verilerin İşlenmesi (Madde 10)	22
2.7. Kimlik Tespiti Gerektirmeyen İşleme (Madde 11)	22
BÖLÜM 3. VERİ SAHİBİNİN HAKLARI	22
3.1. Veri Sahibinin Haklarını Kullanması İçin Şeffaf Bilgilendirme, İletişim ve Yöntemler (Madde 12)	22
3.2. Bilgilendirme	24
3.2.1. Hangi Kişisel Verilerinizi Topluyoruz	24
3.2.2. Bilgilerinizi Nereden Topluyoruz?	24
3.2.3. Bilgilerinizi Neden Topluyoruz?	25
3.2.4. Bilgilerinizi Paylaşma	27
3.2.5. Bilgilerinizi Ne Kadar Süre Saklıyoruz	28
3.3. Erişim Hakkı (Madde 15)	28
3.4. Düzeltme Hakkı (Madde 16)	28
3.5. Silme Hakkı (Unutulma Hakkı) (Madde 17)	28
3.6. İşleme Faaliyetlerini Kısıtlama Hakkı (Madde 18)	29
3.7. Veri Taşıma Hakkı (Madde 20)	30
3.8. İtiraz Hakkı (Madde 21)	30
3.9. Otomatik Karar Verme ve Profil Oluşturmaya İlişkin Hak (Madde 22)	30
3.10. Rızayı Geri Çekme Hakkı	31
3.11. Şikayette Bulunma Hakkı	31
3.12. Veri Koruma Görevlisi	31
3.13. Kısıtlamalar	32
BÖLÜM 4. KONTROLÖR VE İŞLEYİCİ	33
4.1. Kontrolörün Sorumluluğu (Madde 24)	33
4.2. Özel ve Olağan Veri Koruması (Madde 25)	34
4.2.1 Kişisel Verilerin Korunması	34

4.2.2 Özel Nitelikli Kişisel Verilerin Korunması	39
4.3. Ortak Kontrolörler (Madde 26)	40
4.4. Birlik İçerisinde Kurulu Olmayan Kontrolörler veya İşleyicilerin Temsilcileri (Madde 27)	40
4.5. İşleyici (Madde 28)	41
4.6. Kontrolör veya İşleyicinin Yetkisi Kapsamındaki İşleme Faaliyet (Madde 29)	42
4.7. İşleme Faaliyetlerinin Kayıtları (Madde 30)	43
4.8. Denetim Makamıyla İşbirliği (Madde 31)	44
4.9. İşleme Güvenliği (Madde 32)	44
4.10. Bir Kişisel Veri İhlalinin Denetim Makamına Bildirilmesi (Madde 33)	45
4.11. Bir Kişisel Veri İhlalinin Veri Sahibine İletilmesi (Madde 34)	45
4.12. Veri Koruma Etki Değerlendirmesi (Madde 35)	46
4.13. Ön İstişare (Madde 36)	48
4.14. Veri Koruma Görevlisinin Belirlenmesi (Madde 37)	49
4.15. Veri Koruma Görevlisinin Konumu (Madde 38)	49
4.16. Veri Koruma Görevlisinin Görevleri (Madde 39)	50
4.17. Davranış Kuralları (Madde 40)	51
4.18. Onaylı Davranış Kurallarının İzlenmesi (Madde 41)	52
4.19. Belgelendirme (Madde 23)	53
4.20. Belgelendirme Organları (Madde 43)	54
BÖLÜM 5. KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE VEYA ULUSLARARASI KURULUŞLARA AKTARILMASI	56
5.1. Aktarımlar İçin Genel Prensipler (Madde 44)	56
5.2. Yeterlilik Kararına Dayalı Aktarımlar (Madde 45)	59
5.3. Uygun Güvencelere Tabi Aktarımlar (Madde 46)	61
5.4. Bağlayıcı Kurumsal Kurallar (Madde 47)	62
5.5. Sendika Yasalarında İzin Verilmeyen Aktarımlar veya Açıklamalar (Madde 48)	64
5.6. Belirli Durumlar İçin İstisnalar (Madde 49)	65
5.7. Kişisel Verilerin Korunması İçin Uluslararası İşbirliği (Madde 50)	66
5.8. Veri Aktarımı	66
5.8.1. Konsolide Denetim Çerçevesinde	66
5.8.2. Üçüncü Taraflara	67
5.8.3. Hizmet Sağlayıcılara	67
5.8.4. Yetkililere, Düzenleyicilere veya Kamu Kurumlarına	68
5.8.5. Kişisel Verilerin Yurt Dışına Aktarılması	68
BÖLÜM 6. BAĞIMSIZ DENETİM OTORİTELERİ	69

6.1. Denetim Otoritesi (Madde 51)	69
6.2. Bağımsızlık (Madde 52)	70
6.2.1 Makamının Bağımsızlığı	70
6.3. Denetleyici Makam Üyeleri İçin Genel Koşullar (Madde 53)	70
6.4. Denetim Otoritesinin Oluşumuna İlişkin Kurallar (Madde 54)	71
6.5. Yetkinlik (Madde 55)	71
6.6. Baş Denetim Makamının Yeterliliği (Madde 56)	72
6.7. Görevler (Madde 57)	72
6.8. Güçler (Madde 58)	74
6.9. Etkinlik Raporları (Madde 59)	76
BÖLÜM 7. İŞBİRLİĞİ VE TUTARLILIK	76
7.1. Lider Denetim Makamı ile İlgili Diğer Denetim Makamları Arasında İş Birliği (Madde 60)	76
7.2. Karşılıklı Yardımlaşma (Madde 61)	77
7.3. Denetim Makamlarının Ortak Operasyonları (Madde 62)	78
7.4. Tutarlılık Mekanizması (Madde 63)	79
7.5. Yönetim Kurulu'nun Görüşü (Madde 64)	79
7.6. Uyuşmazlıkların Kurul Tarafından Çözülmesi (Madde 65)	81
7.7. Aciliyet Prosedürü (Madde 66)	82
7.8. Bilgi Alışverişi (Madde 67)	82
7.9. Avrupa Veri Koruma Kurulu (Madde 68)	82
7.10. Bağımsızlık (Madde 69)	83
7.11. Kurulun Görevleri (Madde 70)	83
7.12. Raporlar (Madde 71)	85
7.13. Prosedür (Madde 72)	86
7.14. Başkan (Madde 73)	86
7.15. Başkanın Görevleri (Madde 74)	86
7.16. Sekreterlik (Madde 75)	87
7.17. Gizlilik (Madde 76)	87
BÖLÜM 8. ÇÖZÜMLER, SORUMLULUK VE CEZALAR	88
8.1. Bir Denetim Makamına Şikayette Bulunma Hakkı (Madde 77)	88
8.1.1 Şikayet Hakkı:	88
8.1.2. Bilgilendirme ve İlerleme:	88
8.2. Denetim Makamına Karşı Etkili Bir Yargı Yoluna Başvurma Hakkı (Madde 78)	89
8.2.1. Yargı Yolu Hakkı:	89

8.3. Bir Kontrolör veya İşleyiciye Karşı Etkili Bir Yargı Yoluna Başvurma Hakkı (Madde 79)	
89	
8.4. Veri Sahiplerinin Beyanı (Madde 80)	89
8.5. İşlemlerin Askıya Alınması (Madde 81)	90
8.6. Tazminat Hakkı ve Sorumluluk (Madde 82)	90
8.6.1. Tazminat Hakkı Genel İlkeler:	90
8.6.2. Tazminat Talebi İçin Şartlar:	90
8.6.3. İlgili Tarafların Hakları:	91
8.6.4. Uyuşmazlık Çözümü:	91
8.7. İdari Para Cezalarının Uygulanmasına İlişkin Genel Koşullar (Madde 83)	91
8.8. Cezalar (Madde 84)	92
BÖLÜM 9. BELİRLİ İŞLEME DURUMLARI İLE İLGİLİ HÜKÜMLER	93
9.1. İşleme ve İfade ve Bilgi Edinme Özgürlüğü (Madde 85)	93
9.2. Resmi Belgelerin İşlenmesi ve Kamuya Açık Erişim (Madde 86)	94
9.3. Ulusal Kimlik Numarasının İşlenmesi (Madde 87)	94
9.4. İstihdam Bağlamında İşleme (Madde 88)	94
9.5. Kamu Çıkarına Yönelik Arşivleme Amaçları, Bilimsel veya Tarihi Araştırma Amaçları veya İstatistiksel Amaçlarla İşlemeye İlişkin Güvenceler ve İstisnalar (Madde 89)	94
9.6. Gizlilik Yükümlülükleri (Madde 90)	95

BÖLÜM 1. AMAÇ, KAPSAM VE TANIMLAR

AMAÇ

(Madde 1)

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), Avrupa Birliği'nde kişisel verilerin işlenmesi ve korunmasına ilişkin temel kuralları belirleyen bir düzenlemedir. GDPR'ın temel amacı, gerçek kişilerin kişisel verilerinin korunması hakkını güçlendirmek ve bu hakkın tüm AB üye ülkelerinde eşit şekilde uygulanmasını sağlamaktır. Bu amaçla, bireylere kendi kişisel verilerine ilişkin daha fazla bilgi sahibi olma, bu verilerinin nasıl kullanıldığını kontrol etme ve bu verilerinin kötüye kullanılması halinde haklarını arama hakları tanımaktadır.

GDPR, kişisel verilerin işlenmesi ve korunması konusunda aşağıdaki temel ilkeleri belirler:

- Hukuksallık, dürüstlük ve şeffaflık: Kişisel verilerin işlenmesi, ilgili kişinin açık rızasını gerektirir.
- Sınırlı amaçlar: Kişisel veriler, yalnızca belirli ve açıkça belirtilen amaçlar için işlenebilir.
- Veri indirimi: Kişisel veriler, işlendikleri amaç için gerekli olan süre kadar saklanabilir.
- Doğruluk ve tamlık: Kişisel veriler, doğru ve eksiksiz olmalıdır.
- Saklama sınırı: Kişisel veriler, işlendikleri amaçlar için gerekli olduğu sürece saklanabilir.
- Gizlilik: Kişisel veriler, yetkisiz kişilerin erişimine karşı korunmalıdır.
- Veri güvenliği: Kişisel veriler, teknik ve organizasyonel tedbirlerle korunmalıdır.

GDPR'ın temel amacı, Avrupa Birliği'nde kişisel verilerin korunmasını sağlamaktır.

GDPR'ın amaçları şu şekilde özetlenebilir:

- Kişisel verilerin korunmasına ilişkin temel haklar ve özgürlükleri güçlendirmek
- Kişisel verilerin işlenmesini şeffaf ve hesap verebilir hale getirmek
- Kişisel verilerin Avrupa Birliği içinde serbest dolaşımını sağlamak

Bu Politika, kişisel verilerin işlenmesinde gerçek kişilerin korunmasına ilişkin kuralları ve kişisel verilerin serbest dolaşımına ilişkin kuralları düzenlemektedir.

Bu Politika, gerçek kişilerin temel hak ve özgürlüklerini, özellikle de kişisel verilerin korunması hakkını korur.

Banka içinde kişisel verilerin serbest dolaşımı, kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunması ile bağlantılı nedenlerle ne sınırlandırılacak ne de yasaklanacaktır.

Bankamızca kanunda öngörülen temel düzenlemeler doğrultusunda, Banka işleyişi içerisinde kişisel verilerin işlenmesi ve korunması bakımından gerekli idari ve teknik tedbirler alınmakta, gerekli iç prosedürler oluşturulmakta, farkındalığı yükseltilmesi amacıyla gerekli eğitimler düzenlenmekte, çalışanların GDPR süreçlerine uyumları için gerekli tedbirler alınmakta, uygun ve etkin denetim mekanizmaları ile teknolojik altyapı, idari ve hukuki sistem kurulmaktadır.

Bu kanunun amacını anlayarak ve gerekliliklerini yerine getirerek, kişisel verilerin gizliliği ve güvenliğini koruma konusundaki taahhüdümüzü daha etkili bir şekilde yerine getirmeyi hedeflemekteyiz.

KAPSAM

(Madde 2 – 3)

GDPR, Avrupa Birliği'nde yerleşik olan veya Avrupa Birliği'nde faaliyet gösteren, AB'de yerleşik olmayan ancak AB'de yaşayan bireylerin kişisel verilerini işleyen tüm gerçek ve tüzel kişileri kapsamaktadır. GDPR'ın kapsamı, kişisel verilerin işlenmesini ve dolaşımını kapsar.

Bu kapsamda, kişisel verileri işleyen tüm kuruluşlar, GDPR'a uymakla yükümlüdür.

GDPR'ın kapsamına giren kişisel veriler, ad, soyad, kimlik numarası, adres, telefon numarası, e-posta adresi, IP adresi, alışveriş alışkanlıkları, sosyal medya paylaşımları, tarama geçmişi, davranışsal veriler, tıbbi veriler gibi bir kişiyi bir kişiyi doğrudan veya dolaylı olarak tanımlamaya veya onunla iletişime geçmeye elverişli tüm verilerdir.

GDPR'ın kapsamına giren kişisel veriler, AB içinde veya dışında işlenerek dolaşabilir. GDPR'ın kapsamına giren kişisel verilerin işlenmesi, bu verilerin toplanması, kaydedilmesi, saklanması, değiştirilmesi, aktarılması, silinmesi veya yok edilmesi gibi tüm faaliyetleri kapsamaktadır.

GDPR'ın kapsamı şu şekilde özetlenebilir:

- Avrupa Birliği'nde yerleşik veya faaliyet gösteren tüm gerçek ve tüzel kişiler
- Kimlik numarası, adres, telefon numarası, e-posta adresi, IP adresi, alışveriş alışkanlıkları, sosyal medya paylaşımları gibi bir kişiyi tanımlamaya veya onunla iletişime geçmeye elverişli tüm veriler
- Kişisel verilerin toplanması, kaydedilmesi, saklanması, değiştirilmesi, aktarılması, silinmesi veya yok edilmesi gibi tüm faaliyetler

GDPR, kişisel verilerin işlenmesini aşağıdaki şekilde sınıflandırır:

- Kişisel verilerin otomatikleştirilmiş araçlarla işlenmesi: Bu tür işleme, bir kişinin insan müdahalesi olmadan kişisel verilerin işlenmesini ifade eder. Örneğin, bir kişinin alışveriş alışkanlıklarının bir alışveriş sitesi tarafından otomatik olarak analiz edilmesi, kişisel verilerin otomatikleştirilmiş araçlarla işlenmesidir.
- Kişisel verilerin otomatikleştirilmemiş araçlarla işlenmesi: Bu tür işleme, bir kişinin insan müdahalesi ile kişisel verilerin işlenmesini ifade eder. Örneğin, bir kişinin başvuru formunda verdiği bilgilerin bir insan tarafından işlenmesi, kişisel verilerin otomatikleştirilmemiş araçlarla işlenmesidir.

GDPR, kişisel verilerin işlenmesini aşağıdaki şekilde sınırlar:

- Kişisel verilerin işlenmesine ilişkin temel ilkeler: GDPR, kişisel verilerin işlenmesini, yukarıda belirtilen temel ilkelere uygun olarak sınırlar.
- Kişisel verilerin işlenmesine ilişkin gerekçeler: GDPR, kişisel verilerin işlenmesini, açık rıza, sözleşmenin kurulması veya ifası, hukuki yükümlülüklerin yerine getirilmesi, kamu menfaati, meşru menfaat veya temel hak ve özgürlüklere zarar vermemek gibi gerekçelere dayandırır.
- Kişisel verilerin işlenmesine ilişkin sınırlamalar: GDPR, kişisel verilerin işlenmesini, bazı durumlarda, ilgili kişinin açık rızasını almadan da sınırlayabilir. Örneğin, kamu güvenliği, çocuk koruması veya genel sağlık gibi nedenlerle kişisel verilerin işlenmesine izin verilebilir.

GDPR, kişisel verilerin işlenmesini ihlal eden gerçek ve tüzel kişilere, idari para cezası gibi yaptırımlar uygulayabilir.

GDPR'ın kapsamı dışında kalan bazı kişisel veriler şunlardır:

- Kamuya açık olarak erişilebilen kişisel veriler
- İdari veya yargısal işlemlerin yürütülmesi için gerekli olan kişisel veriler
- Tarihi, bilimsel veya arşivsel amaçlarla işlenen kişisel veriler

GDPR, kişisel verilerin işlenmesine ilişkin yeni ve daha sıkı kurallar getirerek, bireylerin kişisel verilerinin korunmasını güçlendirmeyi amaçlamaktadır. GDPR, AB'de kişisel verilerin işlenmesine ilişkin en kapsamlı ve en katı mevzuattır.

İşbu Politika, kişisel verilerin tamamen veya kısmen otomatik yöntemlerle işlenmesi ve bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan kişisel verilerin otomatik araçlar dışında işlenmesi için geçerlidir.

Bu Politika ařağıdaki kiřisel verilerin iřlenmesinde geerli deęildir:

1. Banka hukukunun kapsamı dıřında kalan bir faaliyet sırasında;
2. TEU Bařlık V, Blm 2 kapsamına giren faaliyetleri gerekleřtirirken ye Devletler tarafından;
3. Tamamen kiřisel veya ev ii bir faaliyet sırasında gerek bir kiři tarafından;
4. Kamu gvenlięine ynelik tehditlere karřı koruma ve bu tehditlerin nlenmesi de dahil olmak zere cezai suların nlenmesi, soruřturulması, tespiti veya kovuřturulması veya cezaların infazı amacıyla yetkili makamlar tarafından.

Kiřisel verilerin Banka kurum, ofis ve kuruluřları tarafından iřlenmesi iin 45/2001 sayılı Tzk (AT) uygulanır. 45/2001 sayılı Tzk ve bu tr kiřisel verilerin iřlenmesi iin geerli olan dięer Banka yasal dzenlemeleri, 98. Madde uyarınca bu Politika'nın ilke ve kurallarına uyarlanacaktır.

Bu Politika, 2000/31/EC sayılı Direktifin, zellikle aracı hizmet saęlayıcıların bu Direktifin 12 ila 15. Maddelerindeki sorumluluk kurallarının uygulanmasına halel getirmeyecektir.

Bu Politika, iřlemenin banka iinde gerekleřiř gerekleřmedięine bakılmaksızın, banka iindeki bir kontrolr veya iřleyicinin kuruluřunun faaliyetleri baęlamında kiřisel verilerin iřlenmesine uygulanır.

BİLGE BANK A.ř.

Bu Politika, banka iinde yer alan veri sahiplerinin kiřisel verilerinin, banka iinde yerleřik olmayan bir kontrolr veya iřleyici tarafından iřlenmesine iliřkin olup, iřleme faaliyetleri ařağıdakilerle ilgilidir:

- a. veri sahibinin bir deme yapması gerekip gerekmedięine bakılmaksızın banka iindeki sz konusu veri sahiplerine mal veya hizmetlerin teklif edilmesi; veya
- b. davranıřlarının banka iinde gerekleřmesi halinde davranıřlarının izlenmesi.

Bu Politika, kiřisel verilerin banka iinde yerleřik olmayan ancak uluslararası kamu hukuku uyarınca ye Devlet hukukunun uygulandıęı bir yerde kurulu bir kontrolr tarafından iřlenmesi iin geerlidir.

İřbu Politika'ya uyulmaması veya herhangi bir řekilde iřbu Politika'nın ihlal edilmesi durumunda olayın mahiyetine gre Banka tarafından gerekli yaptırımlar uygulanacak olup, iř akdinin feshine kadar geebilecek disiplin cezaları gndeme gelebilecektir.

Bankamız, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) hükümlerine tam uyum sağlama taahhüdünü taşımaktadır.

TANIMLAR

(Madde 4)

GDPR, kişisel verilerin işlenmesine ilişkin yeni ve daha sıkı kurallar getirerek, bireylerin kişisel verilerinin korunmasını güçlendirmeyi amaçlamaktadır. Bu amaçla, GDPR'da kişisel verilerin işlenmesine ilişkin çeşitli tanımlar yapılmıştır.

GDPR'da yer alan bazı önemli tanımlar şunlardır:

- **Başvuru makamı:** Bireylerin kişisel verilerinin korunması konusundaki şikayet ve taleplerini inceleyip karara bağlayan kamu kuruluşudur. GDPR'a göre, her AB üyesi devlette bir başvuru makamı bulunmalıdır.
- **İşleme:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılması gibi veriler üzerinde gerçekleştirilen her türlü işlemidir.
- **Kişisel veri:** Bir kişiyi doğrudan veya dolaylı olarak tanımlayabilen her türlü bilgidir. Örneğin, ad, soyad, doğum tarihi, adres, telefon numarası, e-posta adresi, IP adresi, davranışsal veriler, tıbbi veriler kişisel veri olarak kabul edilir.
- **Kişisel veri işleme:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılması gibi işlemleri ifade eder.
- **Kişisel verilerin işlenmesi için yasal dayanak:** Kişisel verilerin işlenmesinin hukuka uygun olabilmesi için bir yasal dayanağa dayanması gerekir. Bu yasal dayanaklar, GDPR'ın 6. maddesinde belirtilmiştir. Örneğin, bir web sitesi, kullanıcılarının kişisel verilerini pazarlama amacıyla işlemek için kullanıcılardan açık rıza almalıdır.
- **Kişisel verilerin aktarılması:** Kişisel verilerin, veri sorumlusunun bulunduğu AB üyesi ülke dışındaki bir ülkeye aktarılmasıdır. Kişisel verilerin aktarılması için, GDPR'ın 44. maddesinde belirtilen şartlara uyulması gerekir.
- **Kişisel veri güvenliği:** Kişisel verilerin mevzuata uygun olarak korunmasını ifade eder.
- **Özel nitelikli kişisel veri:** Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli kişisel veri olarak kabul edilir.

- **Rıza:** Bireylerin, kişisel verilerinin belirli bir amaç için işlenmesine açık ve isteğe bağlı bir şekilde onay vermesidir. Bireyin, bilgilendirilmiş olarak ve özgür iradesiyle verdiği rızadır. GDPR'a göre, kişisel verilerin işlenmesine ilişkin rıza, açık, anlaşılır ve kolayca geri alınabilir olmalıdır.
- **Veri sorumlusu (kontrolör):** Kişisel verilerin işleme amaçlarını ve araçlarını belirleyen ve bu amaçlar doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişidir.
- **Veri işleyen:** Veri sorumlusunun verdiği talimatlar doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişidir.
- **Veri sahibi:** Kişisel verileri işlenen gerçek kişidir.
- **Veri güvenliğini ihlal:** Kişisel verilerin mevzuata aykırı olarak işlenmesini, erişilmesini, ifşa edilmesini, değiştirilmesini, yok edilmesini veya kullanılmamasını ifade eder.
- **İhlal Bildirimi (Data Breach Notification):** Veri sorumlularının, önemli bir veri ihlali durumunda, denetleme otoritelerine ve ilgili bireylere bildirimde bulunma yükümlülüğü.
- **Veri Koruma Yetkilisi (Data Protection Officer-DPO):** GDPR'ye göre bazı durumlarda bir kurumun veya kuruluşun veri koruma uzmanı atanması gerekebilir. DPO, veri koruma ile ilgili konularda danışmanlık yapar ve denetler.
- **Veri Konusu (Data Subject):** Kişisel verileri işlenen bireyler, veri konusu olarak adlandırılır.
- **Veri İşleme Kısıtlaması (Data Processing Restriction):** Bir birey, kişisel verilerinin doğruluğunu veya işlenmesinin yasallığını sorguladığında, veri işleme kısıtlaması talep edebilir. Bu, veri işlemenin durdurulmasını içerir.

GDPR'da yer alan diğer tanımlar için, GDPR'ın 4. Maddesinde yer alan aşağıdaki tabloya bakılabilir.

BİLGE BANK A.Ş.

Kişisel Veriler	Tanımlanmış veya tanımlanabilir bir gerçek kişiyle ("veri sahibi") ilgili her türlü bilgi anlamına gelir; Tanımlanabilir bir gerçek kişi, özellikle ad, kimlik numarası, konum verileri, çevrimiçi bir tanımlayıcı gibi bir tanımlayıcıya veya fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğe özgü bir veya daha fazla faktöre atıfta bulunarak doğrudan veya dolaylı olarak tanımlanabilen kişidir.
İşleme	Toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanma, iletme, yayma veya başka bir şekilde yapma yoluyla ifşa etme gibi otomatik yollarla olsun veya olmasın, kişisel veriler veya kişisel veri kümeleri üzerinde gerçekleştirilen herhangi bir işlem veya işlem kümesi anlamına gelir.

	Hizalama veya kombinasyon, kısıtlama, silme veya imha etme kullanılabilir.
İşlemenin Kısıtlanması	Saklanan kişisel verilerin gelecekte işlenmelerini sınırlamak amacıyla işaretlenmesi anlamına gelir.
Profil Oluşturma	Kişisel verilerin bir gerçek kişiyle ilgili belirli kişisel yönleri değerlendirmek, özellikle o gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışı, konum veya hareketleri ile ilgili yönleri analiz etmek veya tahmin etmek için kullanılmasından oluşan kişisel verilerin otomatik olarak işlenmesi anlamına gelir.
Takma Ad	Kişisel verilerin, bu tür ek bilgilerin ayrı tutulması ve kişisel verilerin kendisine atfedilmemesini sağlamak için teknik ve organizasyonel önlemlere tabi olması koşuluyla, ek bilgi kullanılmadan artık belirli bir veri sahibine, tanımlanmış veya tanımlanabilir bir gerçek kişiye atfedilemeyecek şekilde işlenmesi anlamına gelir.
Dosyalama Sistemi	Merkezi, merkezi olmayan, işlevsel veya coğrafi olarak dağılmış olsun, belirli kriterlere göre erişilebilen yapılandırılmış herhangi bir kişisel veri kümesi anlamına gelir;
Denetleyici	Kişisel verilerin işlenmesinin amaç ve araçlarını tek başına veya başkalarıyla ortaklaşa belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer organ anlamına gelir; bu tür işlemlerin amaç ve araçlarının Banka veya Üye Devlet yasaları, denetleyici veya belirli kriterler tarafından belirlendiği durumlarda adaylığı için Banka veya Üye Devlet yasaları tarafından sağlanabilir;
Denetçi	Denetleyici adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya başka bir kurum anlamına gelir.
Alıcı	Üçüncü bir taraf olsun ya da olmasın, kişisel verilerin açıklandığı gerçek veya tüzel kişi, kamu otoritesi, kurum veya başka bir kurum anlamına gelir. Bununla birlikte, Banka veya Üye Devlet yasalarına uygun olarak belirli bir soruşturma çerçevesinde kişisel verileri alabilecek kamu otoriteleri alıcı olarak kabul edilmeyecektir. Bu

	verilerin bu kamu otoriteleri tarafından işlenmesi, işlemenin amaçlarına göre geçerli veri koruma kurallarına uygun olacaktır.
Üçüncü Taraf	Veri sahibi, denetleyici, işleyici ve denetleyicinin veya işleyicinin doğrudan yetkisi altında kişisel verileri işleme yetkisine sahip kişiler dışındaki gerçek veya tüzel kişi, kamu otoritesi, kurum veya kuruluş anlamına gelir.
Rıza	Veri sahibinin 'rızası', beyan veya açık bir olumlu eylemle kendisiyle ilgili kişisel verilerin işlenmesine ilişkin anlaşmayı ifade ettiği isteklerinin serbestçe verilmiş, spesifik, bilgilendirilmiş ve açık bir şekilde belirtilmesi anlamına gelir.
Kişisel Veri İhlali	İletilen, depolanan veya başka şekilde işlenen kişisel verilerin kazara veya yasa dışı olarak imha edilmesine, kaybolmasına, değiştirilmesine, yetkisiz olarak ifşa edilmesine veya bunlara erişilmesine yol açan bir güvenlik ihlali anlamına gelir.
Genetik Verileri	Bir gerçek kişinin kalıtsal veya edinilmiş genetik özelliklerine ilişkin, o gerçek kişinin fizyolojisi veya sağlığı hakkında benzersiz bilgiler veren ve özellikle söz konusu gerçek kişiden biyolojik bir numunenin analizinden kaynaklanan kişisel veriler anlamına gelir.
Biyometrik Veriler	Bir gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin belirli teknik işlemlerden kaynaklanan ve o gerçek kişinin yüz görüntüleri veya daktiloskopik veriler gibi benzersiz tanımlanmasına izin veren veya onaylayan kişisel veriler anlamına gelir;
Sağlıkla İlgili Veriler	Sağlık durumuyla ilgili bilgileri ortaya çıkaran sağlık hizmetlerinin sağlanması da dahil olmak üzere, gerçek bir kişinin fiziksel veya zihinsel sağlığıyla ilgili kişisel veriler anlamına gelir.
Ana Kuruluş	a. Birden fazla Üye Devlette işyerleri bulunan bir kontrolör ile ilgili olarak, kişisel verilerin işlenmesinin amaç ve araçlarına ilişkin kararlar Bankadaki kontrolörün başka bir kuruluşunda alınmadığı ve ikinci kuruluşun bu tür kararları uygulama yetkisine sahip olmadığı sürece, merkezi idaresinin Bankadaki yeri bu durumda, bu tür kararları almış olan kuruluş, ana kuruluş olarak kabul edilmelidir.

	b. Birden fazla Üye Devlette işyerleri bulunan bir işlemciye ilişkin olarak, merkezi yönetiminin Banka içindeki yeri veya, işlemcinin Banka içinde merkezi bir idaresi yoksa, işlemcinin bu Politika kapsamındaki belirli yükümlülüklerle tabi olduğu ölçüde, işlemcinin kuruluş faaliyetleri bağlamında ana işleme faaliyetlerinin gerçekleştiği Banka içinde işlemcinin kurulması.
Temsilci	27. Madde uyarınca denetleyici veya işleyici tarafından yazılı olarak belirlenen, bu Politika kapsamındaki yükümlülükleri bakımından denetleyiciyi veya işleyiciyi temsil eden, Banka içinde kurulmuş gerçek veya tüzel kişi anlamına gelir.
İşletmeler	Düzenli olarak ekonomik faaliyette bulunan ortaklıklar veya dernekler de dahil olmak üzere, yasal biçiminden bağımsız olarak ekonomik faaliyette bulunan gerçek veya tüzel kişi anlamına gelir.
İşletme Grupları	Kontrol eden bir işletme ve onun kontrol edilen işletmeleri anlamına gelir.
Bağlayıcı Kurumsal Kurallar	Bir Üye Devlet topraklarında kurulmuş bir denetleyici veya işlemci tarafından bir grup işletme veya ortak bir ekonomik faaliyette bulunan işletmeler grubu içinde bulunan bir veya daha fazla üçüncü ülkede bir denetleyiciye veya işlemciye kişisel verilerin aktarılması veya aktarılması için uygulanan kişisel veri koruma politikaları anlamına gelir.
Denetim Otoritesi	Bir Üye Devlet tarafından 51. madde uyarınca kurulan bağımsız bir kamu otoritesi anlamına gelir.
İlgili Denetim Otoritesi	<p>Kişisel verilerin işlenmesiyle ilgilenen bir denetim otoritesi anlamına gelir,</p> <ul style="list-style-type: none"> • Denetleyici veya işlemci, söz konusu denetim otoritesinin Üye Devletin topraklarında kurulur; • Söz konusu denetim otoritesinin Üye Devletinde ikamet eden kişisel veriler, işlemde önemli ölçüde etkilenir veya etkilenme olasılığı yüksektir; • Bu denetim otoritesine şikâyetle bulunulabilir.

Sınır Ötesi İşleme	<p>a. Denetleyici veya işlemcinin birden fazla Üye Devlette kurulduğu Bankadaki bir denetleyici veya işlemcinin birden fazla Üye Devletindeki kuruluşların faaliyetleri bağlamında gerçekleşen kişisel verilerin işlenmesi.</p> <p>b. Banka içinde tek bir denetleyici veya işleyici kuruluşunun faaliyetleri bağlamında gerçekleşen, ancak birden fazla Üye Devletteki veri konularını önemli ölçüde etkileyen veya etkilemesi muhtemel olan kişisel verilerin işlenmesi.</p>
İlgili ve Gerekçeli İtiraz	<p>Politikanın ihlal edilip edilmediğine veya denetleyici veya işleyici ile ilgili olarak öngörülen eylemin bu Politikaya uygun olup olmadığına dair bir karar taslağına itiraz anlamına gelir ve bu, veri sahiplerinin temel hak ve özgürlüklerine ve varsa Banka içindeki kişisel verilerin serbest akışına ilişkin karar taslağının ortaya koyduğu risklerin önemini açıkça göstermektedir.</p>
Bilgi Toplumu Hizmeti	<p>Avrupa Parlamentosu ve Konseyi'nin (AB) 2015/1535 sayılı Direktifinin (AB) 1 (1) maddesinin (b) bendinde tanımlanan bir hizmet anlamına gelir.</p>
Uluslararası Organizasyon	<p>Uluslararası kamu hukuku tarafından yönetilen bir kuruluş ve alt organları veya iki veya daha fazla ülke arasındaki bir anlaşma ile veya bu anlaşmaya dayanarak kurulan başka herhangi bir organ anlamına gelir.</p>

GDPR'da yer alan tanımlar, kişisel verilerin işlenmesine ilişkin yeni ve daha sıkı kuralların anlaşılması ve uygulanması için önemlidir.

BÖLÜM 2. PRENSİPLER

2.1. Kişisel Verilerin İşlenmesine İlişkin İlkeler (Madde 5)

Bilge Bank A.Ş. olarak, müşteri gizliliği ve kişisel verilerin korunması konularında taahhütte bulunmaktayız. Bu bağlamda, Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) çerçevesinde kişisel verilerin işlenmesine ilişkin politikamızı aşağıda bulabilirsiniz.

Yasal, Adil ve Şeffaf İşleme:

Kişisel veriler, yasalara uygun, adil ve şeffaf bir şekilde işlenir. İşleme faaliyetlerimiz her zaman mevcut yasal düzenlemelere ve etik standartlara uygundur.

Amaç Sınırlaması:

Veri sahiplerinden topladığımız kişisel veriler, belirli, açık ve meşru amaçlarla toplanır ve bu amaçlar dışında kullanılmaz. Kamu yararı, arşivleme, bilimsel araştırma veya istatistiksel amaçlar doğrultusunda veriler işlenmez.

Veri Minimizasyonu:

Kişisel veriler, işlendikleri amaçla ilgili olarak yeterli, ilgili ve gerekli olanlarla sınırlıdır. Veri minimizasyonu prensibine uygun olarak en az veri kullanılır.

Doğruluk ve Güncellik:

Kişisel veriler, doğru ve güncel tutulur. Yanlış veya eksik veriler, işlendikleri amaç doğrultusunda düzeltilir veya silinir.

Saklama Sınırlaması:

Kişisel veriler, işlendikleri amaç için gerekli olan süreden daha uzun süre tutulmaz. Veri sahiplerinin kimliğini belirlemeye izin verecek şekilde sadece belirli durumlarda ve yasal zorunluluklar çerçevesinde saklanabilir.

Bütünlük ve Gizlilik:

Kişisel veriler, uygun teknik ve organizasyonel önlemlerle korunur. Yetkisiz erişime, yasa dışı işleme ve diğer güvenlik tehditlerine karşı bütünlük ve gizliliği korumak için gerekli önlemler alınır.

Kişisel Veri İşleme Amaçları:

- a. Müşteri hesap yönetimi
- b. Finansal işlemlerin gerçekleştirilmesi
- c. Pazarlama ve tanıtım faaliyetleri

İşlenen Kişisel Veri Kategorileri:

- a. Temel Kimlik Bilgileri: Ad, Soyad, TC Kimlik Numarası
- b. İletişim Bilgileri: Adres, Telefon Numarası, E-posta Adresi
- c. Finansal Bilgiler: Banka Hesap Numarası, Kredi Kartı Bilgileri
- d. Özel Kategorideki Veriler: Sağlık Bilgileri (sadece gerekli durumlarda ve rıza ile)

Veri İşleme Şartları:

- a. Rıza
- b. Sözleşme Yürütme
- c. Hukuki Yükümlülükler
- d. Meşru Menfaat

Veri Paylaşımı ve Aktarımları:

- a. İş Ortağı Kuruluşlar: Müşteri hizmetleri, pazarlama
- b. Üçüncü Parti Firmalar: Bilgi teknolojileri, güvenlik hizmetleri
- c. Denetim Kuruluşları: İlgili yasal düzenlemelere uygun olarak

Veri Güvenliği Tedbirleri:

- a. Şifreleme: Hassas verilerin şifrlenmesi
- b. Güvenlik Duvarları ve Antivirüs Yazılımları: Bilgisayar sistemlerinin korunması
- c. Eğitim Programları: Personelin bilinçlendirilmesi ve eğitilmesi

Kişisel Veri İşleme Şartları:

Bu madde, Bilge Bank'ın kişisel veri işleme süreçlerini gerçekleştirirken rıza, sözleşme, hayati çıkarlar, meşru menfaat ve kamu çıkarları gibi temel yasal şartlara uygun hareket etme taahhütlerini detaylandırmaktadır.

Rıza:

Bilge Bank, kişisel verileri işlemek için rıza alır. Rıza, veri sahiplerine, verilerinin belirli amaçlar doğrultusunda işleneceği, kimlerle paylaşılacağı ve hangi haklara sahip oldukları konularında şeffaf ve anlaşılır bilgi sunularak alınır. Rıza, serbest, bilgilendirilmiş, isteğe bağlı ve açık bir şekilde ifade edilmiş olmalıdır.

Sözleşme:

Bilge Bank, kişisel verileri sözleşme yürütme süreçlerinde işleyebilir. Bu, bir kişi ile Banka arasında bir sözleşmenin kurulması, yürütülmesi veya sonlandırılması amacıyla gerekli olan kişisel verilerin işlenmesini içerir. Sözleşme şartı, işleme amaçlarıyla uygun bir şekilde sınırlıdır ve kişisel verilerin işlenmesi, sözleşme gerekliliklerini yerine getirmek için zorunlu olmalıdır.

Hayati Çıkarlar:

Bilge Bank, kişisel verileri işlemeyi, bir kişinin yaşamını korumak için zorunlu olması durumunda gerçekleştirebilir. Bu durum, acil sağlık durumları veya hayati çıkarlar söz konusu olduğunda geçerlidir. Veri işleme süreçleri, ilgili kişinin veya başka bir kişinin yaşamını korumak için acil bir ihtiyaç doğrultusunda sınırlıdır.

Meşru Menfaat:

Bilge Bank, meşru menfaatleri doğrultusunda kişisel verileri işleyebilir. Meşru menfaat, Bankanın veya üçüncü tarafların haklarını ve özgürlüklerini koruma ihtiyacını içerir ve bu işleme, ilgili kişinin temel hakları ve özgürlükleri üzerinde ağır bir etkisi olmadığı sürece izin verilir. Meşru menfaat temelinde yapılan veri işleme süreçleri her zaman denge ve değerlendirme prensibine tabidir.

Kamu Çıkarları:

Bilge Bank, genel kamu çıkarları veya kamu görevi kapsamında kişisel verileri işleyebilir. Bu durum, Bankanın yasal yükümlülüklerini yerine getirmesi veya kamu hizmeti sağlaması amacıyla gerçekleştirilen veri işleme süreçlerini içerir. Bu çerçevede işlenen veriler, yasal gereksinimlere uygun olarak ve ilgili kamu çıkarlarına hizmet edecek şekilde işlenir.

2.2. İşlemenin Yasallığı (Madde 6)

İşleme yalnızca aşağıdakilerden en az birinin geçerli olması durumunda yasal olacaktır:

- Veri sahibinin kişisel verilerinin bir veya daha fazla özel amaç için işlenmesine izin vermiş olması;
- Veri sahibinin taraf olduğu bir sözleşmenin ifası için veya bir sözleşme yapılmadan önce veri sahibinin talebi üzerine gerekli adımların atılması için işlemenin gerekli olması;
- Veri sorumlusunun tabi olduğu yasal bir yükümlülüğe uymak için işlemenin gerekli olması;
- Veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarının korunması için işlemenin gerekli olması;
- Kamu yararına yürütülen bir görevin yerine getirilmesi veya kontrolöre verilen resmi yetkinin kullanılması için işlemenin gerekli olması;
- Veri sahibinin kişisel verilerin korunmasını gerektiren çıkarları veya temel hakları ve özgürlüklerinin, söz konusu çıkarların, özellikle de verilerin konu bir çocuk.

2.3. Rıza Koşulları (Madde 7)

Rıza ve Şeffaflık:

Veri sahibinin rızası, yazılı bir beyan kapsamında alınabilir. Rıza talebi, diğer hususlardan açıkça ayrılacak şekilde anlaşılır, kolay erişilebilir ve sade bir dilde sunulur. Bu beyan, GDPR'nin ihlalini teşkil eden herhangi bir kısmı bağlayıcı olmaz.

Rıza Geri Çekme Hakkı:

Veri sahibi, herhangi bir zamanda rızasını geri çekme hakkına sahiptir. Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı olarak yapılan işlemlerin hukuka uygunluğunu etkilemez.

Veri sahibi, rıza vermeden önce bu konuda açıkça bilgilendirilecek ve rıza vermek kadar geri çekmek de kolay olacaktır.

2.4. Bilgi Toplumu Hizmetlerine İlişkin Olarak Çocuğun Rızasına İlişkin Koşullar (Madde 8)

Bu madde, Bilge Bank'ın çocuk verilerini işlerken uyguladığı özel önlemleri ve çocukların haklarını koruma taahhütlerini içermektedir.

Çocuk Verisi İşleme Şartları:

Bilge Bank, 16 yaş altındaki çocukların kişisel verilerini işlerken özel bir dikkat ve koruma sağlama taahhüt eder. Çocuk verileri ancak aşağıdaki şartlar altında işlenir:

a. Velinin veya Kanuni Temsilcinin Onayı:

Çocuğun verileri, çocuğun velisi veya kanuni temsilcisi tarafından açıkça onaylanmadıkça işlenmez. Onay, anlaşılır ve erişilebilir bir şekilde sunulmalıdır ve çocuğun anlayış seviyesine uygun olmalıdır.

b. Çocuklara Yönelik Hizmetler İçin Özel İşleme Koşulları:

Çocuklara yönelik ürün ve hizmetlerin sunumu durumunda, Bilge Bank, çocuk verilerini işlerken özel önlemler alır. Bu önlemler, çocukların anlayış seviyelerine uygun dil kullanımını, veri işleme amaçlarını ve yöntemlerini anlayabilecekleri bir şekilde sunmayı içerir.

Çocuk Hakları:

Bilge Bank, çocuklara özel olarak tanınan hakları korur ve destekler. Çocuklar, kendi verilerine erişme, düzeltme, silme ve işleme sınırlama taleplerini rahatlıkla yapabilmelidirler. Bu hakları kullanırken çocukların anlayış seviyeleri göz önünde bulundurulmalıdır.

Çocuk Güvenliği ve Gizliliği:

Bilge Bank, çocukların güvenliği ve gizliliği için gerekli önlemleri alır. Çocuk verileri, yetkisiz erişime, değişikliğe veya ifşaya karşı korunur. Ayrıca, çocuklara yönelik reklamcılık ve pazarlama faaliyetleri özel bir dikkatle ele alınır.

Çocuğa ait kişisel veri rızası -ilişkili olduğu durumlarda:

Bankanın çocuğa ait kişisel verileri işlemek zorunda olduğu durumlarda, velayet sorumluluğunu taşıyan kişi – çocuğun velisi/vasisi olarak kimliğini kanıtlamak ve çocuğun haklarına ilişkin olarak yukarıda belirtilen tüm işlemleri mevzuata uygun olarak, çocuğun reşit yaşına gelmesine kadar yerine getirmesi konusunda mahsus rızasını vermek zorundadır.

2.5. Özel Nitelikli Kişisel Verilerin İşlenmesi (Madde 9)

İrk veya etnik köken, siyasi görüş, dini veya felsefi inanç veya sendika üyeliğini ortaya koyan kişisel verilerin işlenmesi ile genetik verilerin, biyometrik verilerin, bir gerçek kişiyi benzersiz şekilde tanımlamak amacıyla, sağlıkla ilgili veriler veya gerçek kişiye ilişkin verilerin işlenmesi kişinin cinsel yaşamı veya cinsel yönelimi yasaktır. Fakat bu madde, aşağıdakilerden biri geçerli olduğunda uygulanmaz:

- Veri sahibi, belirli bir veya birkaç belirlenmiş amaç için kişisel verilerin işlenmesine açık rıza vermişse, ancak Birlik veya Üye Devlet hukuku, 1. paragrafta bahsedilen yasağın veri sahibi tarafından kaldırılamayacağını belirtiyorsa;
- İşleme, istihdam, sosyal güvenlik ve sosyal koruma hukuku alanında kontrolörün veya veri sahibinin belirli haklarının yerine getirilmesi ve kullanılması amacıyla Birlik veya Üye Devlet hukuku veya Üye Devlet hukukuna uygun olarak sağlanan bir toplu sözleşme tarafından yetkilendirilmişse;
- İşleme, veri sahibinin fiziksel veya hukuki olarak rıza verme yeteneğinin olmadığı durumlarda, veri sahibinin veya başka bir doğal kişinin hayati çıkarlarını korumak için gerekliyse;
- İşleme, politik, felsefi, dini veya sendika amaçları olan bir vakıf, dernek veya diğer kâr amacı gütmeyen bir kuruluş tarafından uygun korumalarla gerçekleştirilir ve işleme yalnızca kuruluşun üyeleri veya eski üyeleri veya amaçları doğrultusunda düzenli teması olan kişilere ilişkinse ve kişisel veriler bu kuruluş dışında veri sahiplerinin rızası olmadan açıklanmaz;
- İşleme, veri sahibi tarafından açıkça kamuoyuna açıklanan kişisel verilere ilişkinse;
- İşleme, hukuki iddiaların tesis edilmesi, kullanılması veya savunulması veya mahkemelerin yargı yetkisi çerçevesinde faaliyet gösterdiği durumlarda;
- İşleme, Birlik veya Üye Devlet hukukuna dayanarak, amaçlanan amaçla orantılı olan, veri koruma hakkının özünü saygı gösteren ve veri sahibinin temel haklarını ve çıkarlarını korumak için uygun ve özel tedbirleri öngören, önemli bir kamu yararı nedeniyle gerekliyse;
- İşleme, Birlik veya Üye Devlet hukuku uyarınca sağlık profesyoneli ile yapılan bir sözleşme veya bir sözleşmeye dayanarak, önleyici veya işyeri tıbbı, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık veya sosyal bakım veya tedavi

veya sađlık veya sosyal bakım sistemlerinin ve hizmetlerinin yönetimi amacıyla gerekiyorsa ve 3. paragrafta belirtilen kořullar ve korumalar altında;

- i. İşleme, bir kamu sađlığı alanındaki kamu yararı nedeniyle, ciddi sınır ötesi sađlık tehditlerine karşı koruma veya sađlık hizmetlerinin ve tıbbi ürünlerin veya tıbbi cihazların kalite ve güvenliği konusunda yüksek standartların sađlanması gibi nedenlerle Birlik veya Üye Devlet hukuku uyarınca sađlanan uygun ve özel tedbirleri öngören durumlarda;
- j. İşleme, Birlik veya Üye Devlet hukukuna dayanarak, kamu yararı için arşivleme amacıyla, bilimsel veya tarihsel araştırma amacıyla veya istatistiksel amaçlarla yapılıyorsa ve 89(1) maddeye dayanılarak, amaçlanan amaçla orantılı olan, veri koruma hakkının özünü saygı gösteren ve veri sahibinin temel haklarını ve çıkarlarını korumak için uygun ve özel tedbirleri öngörüyorsa.

2.6. Ceza Mahkûmiyeti ve Suça İlişkin Kişisel Verilerin İşlenmesi (Madde 10)

İşlemenin yasallığı uyarınca ilgili güvenlik önlemleriyle ilgili kişisel verilerin işlenmesi, yalnızca resmi makamın kontrolü altında veya işleme, Veri sahiplerinin hakları ve özgürlükleri. 2 Cezai hükümlere ilişkin kapsamlı kayıtlar yalnızca resmi makamın kontrolü altında tutulacaktır.

2.7. Kimlik Tespiti Gerektirmeyen İşleme (Madde 11)

Veri İşleme Amaçları:

Kişisel verilerin işlenme amaçları, başlangıçta tanımlandığında ve geçerli olduğunda belirtilir. Ancak, bu amaçlar artık geçerli değilse veya veri sahibinin tanımlanması artık gerekmiyorsa, kontrolör, veri sahibini bilgilendirir ve yeni amaçları açıkça belirtir.

Veri Sahibi Bilgilendirmesi:

Bu durumda, kontrolör, veri sahibini mümkünse bu değişiklik hakkında bilgilendirir. Ancak, kontrolör veri sahibini tanımlayabilecek durumda değilse, bu durumu gösterir ve veri sahibine bu durumu bilmeksizin bu madde kapsamındaki haklarını kullanmak için ek bilgi sağlaması gerektiğini belirtir.

Hakların Kullanımı:

Bu tür durumlarda, Veri Koruma Kanunu'nun 20. maddesi, veri sahibinin kimliğini belirleme amacını taşımadıkça geçerli olmayacaktır. Veri sahibi, bu haklarını kullanmak için ek bilgi sağlamak amacıyla gerekli adımları atmalıdır.

BÖLÜM 3. VERİ SAHİBİNİN HAKLARI

3.1. Veri Sahibinin Haklarını Kullanması İçin Şeffaf Bilgilendirme, İletişim ve Yöntemler (Madde 12)

- Veri kontrolörü, veri sahibine yönelik her türlü bilginin açık, anlaşılır ve kolay erişilebilir bir şekilde sağlanması için uygun tedbirleri almalıdır, özellikle çocuklar için bu bilgiler daha da özenle sunulmalıdır. Bilgiler, yazılı veya elektronik olarak sağlanabileceği gibi, veri sahibi tarafından talep edilirse sözlü olarak da sağlanabilir.
- Veri kontrolörü veri sahibi haklarının kullanılmasını kolaylaştırır. Veri kontrolörü veri sahibinin kimliğini belirleyebilecek konumda olmadığını göstermedikçe, kontrolör veri sahibinin 15 ila 22. maddeler kapsamındaki haklarını kullanma talebi üzerine harekete geçmelidir.
- Veri kontrolörü 15 ila 22. maddeler kapsamındaki bir talep üzerine gerçekleştirilen işlemlere ilişkin bilgileri gereksiz gecikme olmaksızın ve her halükarda talebin alınmasını müteakip **bir ay** içerisinde veri sahibine sağlar. Bu süre, taleplerin karmaşıklığı ve sayısı dikkate alınarak, gerekli hallerde **iki ay** daha uzatılabilir. Kontrolör talebin alınmasından itibaren bir ay içerisinde, gecikmenin nedenleri ile birlikte, veri sahibini bu tür bir uzatma konusunda bilgilendirir. Veri sahibinin elektronik form vasıtasıyla talepte bulunduğu hallerde, veri sahibi tarafından aksi talep edilmedikçe, bilgiler mümkün olan hallerde elektronik yollarla sağlanır.
- Veri kontrolörünün veri sahibinin talebi üzerine harekete geçmemesi halinde, kontrolör gecikmeksizin ve talebin alınmasından itibaren en geç bir ay içerisinde veri sahibini harekete geçmeme nedenleri ve bir denetim makamına şikayette bulunma ve yargı yoluna başvurma olasılığı hakkında bilgilendirir.
- Madde 13 ve 14 kapsamında sağlanan bilgiler ve madde 15 ila 22 ve 34 kapsamında gerçekleştirilen her türlü iletişim ve eylem ücretsiz olarak sağlanır. Bir veri sahibinden gelen taleplerin özellikle tekrar eden nitelikleri nedeniyle açıkça temelsiz veya aşırı olduğu hallerde, kontrolör

a) bilgi veya iletişimin sağlanması ya da talep edilen eylemin gerçekleştirilmesine ilişkin idari maliyetler dikkate alınarak makul bir ücret talep edebilir.

b) talebi reddedebilir.

Talebin açıkça temelsiz veya aşırı nitelikte olduğunu gösterme yükü kontrolöre aittir.

- Kontrolörün 15 ila 21. maddelerde atıfta bulunulan talepte bulunan gerçek kişinin kimliğine ilişkin makul şüphelerinin bulunması halinde, 11. maddeye halel gelmeksizin, kontrolör veri sahibinin kimliğinin teyit edilmesi için gerekli ek bilgilerin sağlanmasını talep edebilir.
- 13 ve 14. maddeler uyarınca veri sahiplerine sağlanacak bilgiler, amaçlanan işleme faaliyetine ilişkin anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve açıkça okunabilir bir şekilde sunulması amacıyla standartlaştırılmış simgeler ile birlikte sağlanabilir.
- Simgelerin elektronik olarak sunulduğu hallerde, bunlar makine tarafından okunabilir olacaktır.
- Komisyon, simgeler tarafından sunulacak bilgilerin ve standartlaştırılmış simgelerin sağlanmasına ilişkin usullerin belirlenmesi amacıyla 92. madde uyarınca yetki devrine dayalı tasarruflar kabul etme yetkisine sahiptir.

3.2. Bilgilendirme

Veri Koruma Yasaları uyarınca, kişisel bilgilerinizi yalnızca aşağıda belirtilenler gibi uygun bir nedenimizin olması durumunda işleyebiliriz:

- Bunu yapmak kendi meşru çıkarlarımıza uygun olduğunda
- Yasal bir zorunluluk halinde
- Bizimle bir finansal ürün veya hizmet için sözleşme imzaladığınızda
- Kişisel bilgilerinizi işlememiz için bize onay verdiğinizde

Aşağıdakilere halel getireceği ölçüde verileri saklayabiliriz:

- Finansal hizmetler yasalarının ihlallerinin önlenmesi, tespiti veya soruşturulması ya da uygulanması
- Banka tarafından yürütülen bir süreç, prosedür, inceleme, soruşturma, değerlendirme, başvuru veya uzlaşma
- Finansal hizmet sağlayıcılarının düzenlenmesi
- Ticari faaliyetler yürütülmesi
- Hizmetlerin sunulması
- Ürünlerin satışı
- Müşteri ilişkileri yönetimi
- Pazarlama faaliyetleri
- Araştırma ve geliştirme faaliyetleri
- Hukuk ve güvenlik

3.2.1. Hangi Kişisel Verilerinizi Topluyoruz

Sipariş ettiğiniz veya ilgilendiğiniz hizmetlere bağlı olarak aşağıdakiler de dahil olmak üzere farklı türde kişisel verileri topluyor ve işliyoruz:

- Temel kişisel verileriniz, örneğin adınız ve iletişim bilgileriniz

- Mali bilgileriniz, örneğin kredi notunuz veya geçmişiniz..
- Eğitiminiz, mesleğiniz veya işinizle ilgili veriler.
- Aileniz ve diğer ilişkileriniz hakkında bilgi.
- Sizlere sunduğumuz hizmet ve ürünler ile bunlara yönelik tercihlerinize ilişkin ayrıntılar.

3.2.2. Bilgilerinizi Nereden Topluyoruz?

Sizin hakkınızda bize sağladığınız veya başka bir yerden topladığımız/aldığımız aşağıdaki gibi kişisel ve mali bilgileri saklıyoruz:

- Başvuru formlarında bize verdiğiniz bilgiler;
- Hesaplarınızı nasıl kullandığımızdan elde ettiğimiz bilgiler;
- Size kimin mal ve hizmet sağladığına ilişkin ayrıntılar;
- Kredi referansı ve dolandırıcılığı önleme kurumları gibi diğer kuruluşlardan alınan bilgiler;
- Ortak hesap sahipleri ve finansal olarak bağlantılı olduğunuz kişiler gibi sizi tanıyan kişilerden alınan bilgiler; Ve
- Mali incelemeler ve görüşmeler sırasında diğer kişilerin (danışmanlarınız gibi) bize verdiği bilgiler ve bankacılık işlemlerinizi analiz ederek elde ettiğimiz bilgiler

Hakkınızda tuttuğumuz bilgilerin sağlığını, ırkınız veya etnik geçmişiniz, cinsel yaşamınız, cezai mahkumiyetleriniz, biyometrik verileriniz veya yasal işlemlerinizi ilgili bilgiler gibi hassas kişisel verileri kapsadığı zamanlar olabilir. Bu tür verileri yalnızca size sunduğumuz ürün veya hizmetlerin amaçları doğrultusunda ihtiyaç duyduğumuzda işleriz. İşlemenin gerekli olmadığı ve kanunen buna izin verilmediği sürece (örneğin, mali suçları tespit etmek ve önlemek amacıyla) hassas verileri işlemek için her zaman açık onayınızı isteyeceğiz.

İşlemenin rızaya dayalı olması durumunda, işlemi istediğiniz zaman geri çekebilirsiniz. Onayınızı geri çekerseniz size belirli hizmetleri veya ürünleri sağlayamayabileceğimizi lütfen unutmayın.

Bu bildirimin sonunda yer alan iletişim bilgilerini kullanarak bizimle iletişime geçerek onayınızı istediğiniz zaman geri çekebilirsiniz.

Hizmetimizin beklentilerinizi her zaman karşılamasını istiyoruz ve bu nedenle hakkınızda tuttuğumuz bilgilerin doğru ve güncel olmasına ihtiyacımız var. Kişisel bilgilerinizde herhangi bir değişiklik olması durumunda lütfen hemen bize bildirerek bize yardımcı olun. Sizin için sahip olduğumuz iletişim bilgilerini e-Bankacılık veya Bölge aracılığıyla veya şubeniz veya Hesap Yöneticiniz ile iletişime geçerek kontrol edebilirsiniz. E-posta adresiniz veya cep telefonu numaranız da dahil olmak üzere iletişim bilgilerinizdeki değişiklikleri bize bildirmeniz önemlidir.

3.2.3. Bilgilerinizi Neden Topluyoruz?

Ürün ve hizmetleri yönetmek için: Bilge Bank'ta hesaplarınızı yönetmek ve ihtiyaçlarınıza uygun hizmetler sunmak için bilgilerinizi saklıyor ve kullanıyoruz. Buna ödemeler, müşteri tavsiyeleri, müşteri hizmetleri, müşteri yönetimi, kredi değerlendirmesi ve pazarlamanın yanı sıra yasal yükümlülüklerle uyum da dahildir.

Kimlik doğrulama için: Bize sağladığınız kişisel bilgileri, mali suçları ve kara para aklamayı önlemek ve tespit etmek amacıyla kimliğinizi, yaşıınızı ve ikametgahınızı doğrulamak için kullanacağız. Kara Para Aklamayı Önleme mevzuatı uyarınca, hem bir bankacılık hizmetine ilk başvurduğunuzda hem de sürekli olarak kimliğinizin doğrulanmasını istemek konusunda yasal yükümlülüğümüz bulunmaktadır. Bunu yapmak için elektronik doğrulama sağlayan ticari bir üçüncü taraf kullanıyoruz.

Ürün veya hizmetlerin uygunluğunu değerlendirmek: Bilgilerinizi, hakkınızda kredi kararları vermek de dahil olmak üzere, ürünlerimizin ve hizmetlerimizin sizin için uygun olup olmadığını değerlendirmek için kullanacağız. Bu, riskle ilgili yönetim bilgileri üretmek için kredi puanlamayı ve düzenli istatistiksel analizleri içerecektir.

Grup içindeki başka bir hesap sahibine finansal olarak bağlıysanız, bağlantılı olduğunuz kişinin kredi başvurusunu onaylayıp onaylamamaya karar verirken, söz konusu kişinin bağlı olduğu bir işletme adına başvuruda bulunması da dahil olmak üzere, bilgilerinize bakacağız. Gruptaki şirketlerin tam listesi için lütfen şubenizle iletişime geçin veya Veri Koruma Görevlisine yazın:

Veri Koruma Görevlisi: Bilge Bank A.Ş.

Adres: Refik Saydam Cad. No:39 Şişhane, Beyoğlu – İstanbul Bilge Bank A.Ş.

Telefon: +90 216 00 00

Fax: +90 216 00 01

Web Adresi: www.bilgebank.com.tr

Kep Adresi: bilgebank@hs01.kep.tr

Dolandırıcılığın önlenmesi veya borcun tahsil edilmesi: Bilgilerinizi dolandırıcılığı önlemek ve borçları kurtarmak için kullanacağız. Bir krediye veya kredi almanızı sağlayan bir ürüne başvurduğunuzda karar vermemize yardımcı olmaları için kredi referansı ve dolandırıcılığı önleme ajanslarını kullanacağız.

Yanlış veya yanlış bilgi vererseniz ve dolandırıcılık yaptığınızı tespit edersek bilgilerinizi dolandırıcılığı önleme kurumlarına iletacağız. Dolandırıcılık tespit edilirse belirli hizmetler, finansman veya istihdam reddedilebilir.

Kolluk kuvvetleri de bu bilgilere erişecek ve bunları kullanacak. Biz ve diğer kuruluşlar, örneğin aşağıdaki durumlarda dolandırıcılığı önlemek için bu bilgilere erişecek ve bunları kullanacağız:

Kredi ve krediye ilgili hesaplar veya diğer olanaklara ilişkin başvurulara ilişkin ayrıntıların kontrol edilmesi;

- Kredi ve krediye ilgili hesapları veya tesisleri yönetmek;
- Borcun kurtarılması;
- Her türlü sigortaya ilişkin teklif ve taleplere ilişkin ayrıntıların kontrol edilmesi,
- İş başvurusunda bulunanların ve çalışanların ayrıntıları kontrol edilir.

İlgili dolandırıcılık önleme kurumlarının bilgilerini almak istiyorsanız lütfen şubenizle iletişime geçin veya bu bildirimin sonundaki iletişim bilgilerini kullanın.

Biz ve diğer kuruluşlar, diğer ülkelerdeki dolandırıcılık önleme kuruluşları tarafından kaydedilen bilgilere de erişiyor ve bunları kullanıyoruz.

Size kredi vermeden önce kredi referans acentelerini kullanarak kredi araştırmaları gerçekleştireceğiz. Bu kontroller, sizinle krediye ilgili ürün veya hizmetlere ilişkin bir sözleşme imzalamadan önce gereklidir. Sizinle olan iş ilişkimiz sırasında, sorumlu kredilendirmeyi ve basiretli hesap yönetimini teşvik etmeye yönelik meşru menfaatlerimizin bir parçası olarak bilgilerinizi kredi referans kuruluşlarıyla da paylaşacağız.

Müşterilerimizi korumak için: Bilgilerinizi sizi korumak için aşağıdaki şekillerde kullanırız:

- Görüşmelerimizin ayrıntılarını doğrulamak, güvenliğinizi için, personelimizi eğitmek ve hizmet kalitemizi korumak için telefon görüşmelerini kaydediyor veya izliyoruz.
- Suçu önlemek ve tespit etmek amacıyla tesislerimizin içindeki ve çevresindeki görüntüleri kaydetmek
- Dolandırıcılık ve mali suçları önlemek ve korumak için müşteri hesaplarındaki işlemleri davranışsal biyometri kullanarak analiz edeceğiz

Kişisel bilgilerinizi bu şekilde kullanmak, yasal yükümlülüklerimize uymamıza ve meşru çıkarlarımızı karşılamamıza olanak tanır.

Araştırma nedenleri: Bilgilerinizi ayrıca araştırma amacıyla kullanacağız ve satın alma tercihlerinizi anlamak için profil oluşturma dahil otomatik karar almayı üstleneceğiz.

Kişisel bilgilerinizi bu şekilde kullanmak, meşru çıkarlarımızı karşılamak için ürünlerimizi ve hizmetlerimizi geliştirmemize, iyileştirmemize ve pazarlamamıza olanak tanır.

3.2.4. Bilgilerinizi Paylaşma

Hesaplarınızı yönetmenize yardımcı olmak için başkalarına bilgi vermemiz gereken başka durumlar da vardır. Bunu hem sizin hem de bizim çıkarlarımıza uygun olduğunda yaparız. Bu durumları aşağıda belirtilmiştir.

- Sizin adınıza hareket etmesi için atadığınız veya yetkilendirdiğiniz birine hakkınızda bilgi verebiliriz.
- Sizi, size ürün ve hizmet sağlayan üçüncü taraflara yönlendirirsek bilgilerinizi bu taraflara aktarmamız gerekir. Verdiğimiz bilgilerin kaydını tutacaklar.
- Kredi riskini değerlendirmek, dolandırıcılığı önlemek veya riski yönetmek veya hesaplarınızı yönetmemize yardımcı olmak için Gruptaki diğer şirketlerle hakkınızda bilgi alışverişinde bulunabiliriz. Hizmetlerimizi geliştirebilmemiz amacıyla araştırma

hazırlamak ve istatistikleri analiz etmek (risk ve kredi analizi dahil) amacıyla da bilgilerinizi Grup içinde paylaşabiliriz.

- Hizmet sağlayıcılar, acenteler ve alt yüklenicilerin bizim adımıza hizmet sağlaması ve bilgilerinizi işlemesi için ayarlamalar yaparız. Bu hizmet sağlayıcıların, acentelerin ve alt yüklenicilerin bilgilerinizi gizli ve güvende tutma görevine sahip olmasını ve bilgilerinizi yalnızca yazılı bir sözleşmede belirtildiği şekilde işlemelerini sağlayacağız.
- Düzenleyicilere karşı görevlerimizi yerine getirmek amacıyla, raporlama, uyumluluk ve denetim amacıyla yetkili kişilerin (sizinle ilgili bilgileri içerecek olan) kayıtlarımızı görmesine izin vereceğiz.
- Ödeme Hizmetleri Düzenlemeleri kapsamındaki yasal yükümlülüklerimizi yerine getirmek amacıyla, hesabınıza yapılan bir ödemenin iade edilmesi yönünde bir talep alırsak ve Ödemeyi Yapan, bankasına ödemenin yanlışlıkla yapıldığını bildirmişse, bunu makbuz üzerine iade etmeliyiz. Yazılı bir talep üzerine, ödeme yapan kişinin sizden paranın geri ödenmesini talep edebilmesi için ödeme yapan kişiye ilgili tüm bilgileri sağlayın. Bu, adınızı ve adresinizi ödemeyi yapan kişinin bankasına verebileceğimiz anlamına gelir. Alacaklının bankası, adınızı ve adresinizi alacaklıya açıklamadan önce sizi bilgilendirmelidir.
- Ayrıca yasaların gerektirmesi halinde, kamu kurumlarıyla bilgi paylaşımı yapılabilir.

3.2.5. Bilgilerinizi Ne Kadar Süre Saklıyoruz

Bilge Bank müşterisi olduğunuz sürece kişisel bilgilerinizi saklayacağız.

- Aşağıdaki nedenlerden dolayı müşteri olmayı bıraktıktan sonra da, siz silme/ anonimleştirme talebi oluşturana kadar verilerinizi 7 yıla kadar saklayacağız:
- Bir şikayete yanıt vermek veya size adil davranıp davranmadığımızı göstermek için;
- Müşteri verilerini araştırma amacıyla analiz etmek;
- Yasal veya düzenleyici gerekliliklere uymak.

3.3. Erişim Hakkı (Madde 15)

Banka olarak hakkınızda sakladığımız ve işlediğimiz bilgilere erişme ve bu bilgilerin nereden geldiğini ve ne için kullandığımızı öğrenme hakkına sahipsiniz. Ayrıca bilgilerinizi ne kadar süreyle sakladığımız ve bilgilerinizi kimlerle paylaştığımız konusunda bilgi alma hakkına da sahipsiniz. Ancak erişim hakkınız kanunlar, başka bir kişinin mahremiyetinin korunması ihtiyacı veya bankanın ticari iş stratejileri ve operasyonlarının değerlendirilmesi nedeniyle kısıtlanabilir. Verilerinize erişim genellikle ücretsiz olarak sağlanacaktır, ancak bazı durumlarda Veri Koruma Yasaları uyarınca bunu yapmaya yetkili olduğumuz durumlarda küçük bir ücret talep edebiliriz.

3.4. Düzeltme Hakkı (Madde 16)

Hakkınızda tuttuğumuz bilgilerin yanlış veya eksik olduğunu düşünüyorsanız bizden bilgilerinizi düzeltmemizi isteme hakkı.

Veri sahibi, kendisi ile ilgili yanlış kişisel verilerin herhangi bir gecikme olmaksızın kontrolörden düzeltilmesini talep etme hakkına sahiptir. İşlemenin amaçları dikkate alındığında, veri sahibi, ek bir beyanda bulunmak da dahil olmak üzere, eksik kişisel verileri tamamlama hakkına sahip olacaktır.

3.5. Silme Hakkı (Unutulma Hakkı) (Madde 17)

Bilgilerinizi kullanmamıza itiraz etme veya saklamamıza gerek yoksa silmemizi, kaldırmamızı veya saklamayı durdurmamızı isteme hakkı. Buna 'itiraz hakkı', 'silinme hakkı' veya 'unutulma hakkı' deniyor. Ancak bilgilerinizi saklamamız veya kullanmamız için yasal veya düzenleyici nedenler olabilir. Bazen bilgilerinizin kullanımını, yalnızca yasal talepler için veya yasal hakların kullanılması amacıyla kullanılacak şekilde kısıtlayabiliriz. Bu durumlarda, bilgilerinizi kısıtlı olduğu sürece kullanmayız veya paylaşmayız.

Aşağıdaki durumlarda veri sahibinin talep ettiği kişisel verilerin işlenmesi, söz konusu kişisel verilere yönelik tüm bağlantıların veya bunların kopyalanmasının veya çoğaltılmasının söz konusu kontrolörler tarafından silinmesi.

- kişisel verilerin toplanma veya başka şekilde işlenme amaçlarıyla bağlantılı olarak artık gerekli olmaması;
- işleme faaliyetinin dayandığı rızayı geri çekmesi ve işleme için başka bir hukuki dayanağın bulunmaması;
- işlemeye itiraz etmesi ve işleme için herhangi bir ağır basan meşru gerekçenin bulunmaması
- kişisel verilerin hukuka aykırı olarak işlenmiş olması;
- Veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukukundaki yasal bir yükümlülüğe uygunluk açısından kişisel verilerin silinmesinin zorunlu olması

3.6. İşleme Faaliyetlerini Kısıtlama Hakkı (Madde 18)

Veri sahibi, aşağıdakilerden birinin geçerli olduğu durumlarda kontrolörden işleme kısıtlaması alma hakkına sahip olacaktır:

- Kişisel verilerin doğruluğuna veri sahibi tarafından, kontrolörün kişisel verilerin doğruluğunu doğrulamasını sağlayacak bir süre boyunca itiraz edilmesi;
- İşlemenin hukuka aykırı olması ve veri sahibinin kişisel verilerin silinmesine karşı çıkması ve bunun yerine kullanımının kısıtlanmasını talep etmesi;
- Kontrolörün artık işleme amaçları doğrultusunda kişisel verilere ihtiyacı yoktur ancak veri sahibi tarafından yasal iddiaların oluşturulması, uygulanması veya savunulması için bunlara ihtiyaç duyulur;
- Veri sahibi , kontrolörün meşru gerekçelerinin veri sahibinin meşru gerekçelerine üstün gelip gelmediğinin doğrulanmasını bekleyen Madde 21 (1) uyarınca işleme faaliyetine itiraz etmişse

İşlemenin kısıtlandığı durumlarda, bu tür kişisel veriler, saklama haricinde, yalnızca veri sahibinin rızası ile veya yasal taleplerin oluşturulması, uygulanması veya savunulması veya başka bir gerçek veya başkasının haklarının korunması amacıyla işlenecektir. (Tüzel kişi veya Birliğin veya bir Üye Devletin önemli kamu çıkarını ilgilendiren nedenlerden dolayı.) işleme kısıtlaması alan veri sahibi, işleme kısıtlaması kaldırılmadan önce kontrolör tarafından bilgilendirilir.

Bu hak size kişisel verilerinizin Bilge Bank tarafından işlenmesini kısıtlama hakkı verir. Bu hakkın kullanıldığı durumlarda, Bilge Bank'ın kişisel verilerinizi saklamasına izin verilmekle birlikte, belirli sınırlı durumlar haricinde verilerin başka şekillerde kullanılması yasaktır.

Aşağıdakilerden birinin geçerli olması durumunda bu hakkınızı kullanabilirsiniz:

- Hakkınızda tutulan kişisel verilerin doğruluğuna itiraz ediyorsunuz ve Bilge Bank bu verilerin doğruluğunu teyit ediyor
- Kişisel verilerin hukuka aykırı olarak işlenmiş olması ve silinmesine karşı çıkıyor ve bunun yerine kısıtlanmasını talep ediyorsunuz
- Bilge Bank'ın artık kişisel verilere ihtiyacı yok ancak siz bu verilere yasal bir taleple bağlantılı olarak ihtiyacınız var
- İşleme işlemine itiraz ettiniz ve Bilge Bank, meşru gerekçelerinin sizin hak ve çıkarlarınıza üstün gelip gelmediğini değerlendiriyor.

3.7. Veri Taşıma Hakkı (Madde 20)

Bu hak, kişisel verilerinizi, Merkez Bankasının kişisel verilerinizi rızaya dayalı olarak veya bir sözleşmenin ifası ve işlemenin gerçekleştirilmesi halinde işlediği başka bir kuruluşa aktarabilmenizi sağlayacak formatta elde etmenize olanak tanır. Otomatik yollarla yapılır. Teknik olarak mümkün olması halinde, kişisel verilerinizin tarafımızdan doğrudan diğer kuruluşa aktarılmasını sağlama hakkına sahip olabilirsiniz .

Uygulanabilirlik:

Bu hak, kişisel verilerin yasal bir yükümlülüğe uyum amacıyla veya kamu yararına yürütülen bir görevin yerine getirilmesi veya resmi yetkinin kullanılması amacıyla gerekli olduğu durumlarda geçerli değildir. Dolayısıyla bu hak, Bilge Bank'ın yasal işlevlerini yerine getirirken elinde bulundurduğu kişisel verilerin çoğu için geçerli değildir.

3.8. İtiraz Hakkı (Madde 21)

Belirli durumlarda bankamızın kişisel verilerinizi kullanmasına itiraz etme hakkınız bulunmaktadır. Ancak bankamız, itirazınıza rağmen, zorlayıcı meşru nedenlerin bulunması veya kişisel verilerinizi herhangi bir hukuki taleple bağlantılı olarak kullanmamızın gerekli olması halinde, kişisel verilerinizi kullanmaya devam edebilir.

Uygulanabilirlik:

Bu hak, bankamızın kişisel verilerinizi kamu yararına yürütülen bir görevin yerine getirilmesi veya resmi yetkinin kullanılması veya meşru menfaatleri doğrultusunda işlenmesi halinde geçerlidir.

3.9. Otomatik Karar Verme ve Profil Oluşturmaya İlişkin Hak (Madde 22)

Kararın yasal bir etki yaratması veya sizi önemli ölçüde etkilemesi halinde, yalnızca otomatik işlemeye dayalı (insan müdahalesi olmadan) bir karara tabi olmama hakkına sahipsiniz.

Bilge Bank, kredi veya kredi kartı başvurularını onaylamak, dolandırıcılığı önlemek ve profil oluşturma durumunda tercihlerinizi karşılayan belirli hizmetleri ve ürünleri size sunabilmek ve pazarlamamızı hedeflemek için profil oluşturma da dahil olmak üzere otomatik karar alma mekanizmasını kullanır. Yasal haklarınızı etkilediği veya üzerinizde olumsuz etkisi olduğu (örneğin, çevrimiçi bir kredi başvurusunun reddedilmesi) durumlarda otomatik karar alma sürecine tabi olmama hakkına sahipsiniz.

Ayrıca bilgilerinizi pazarlama amaçlı profil oluşturma amacıyla kullanmayı bırakmamızı isteme hakkına da sahipsiniz. Verilerinizi işlememiz için bize onay verdiyseniz ve işleme otomatik olarak gerçekleştiyse, kişisel bilgilerinizi bizden kolayca yeniden kullanılabilir elektronik bir formatta alma hakkına sahipsiniz. Ayrıca bilgilerinizi bu formatta diğer kuruluşlara aktarmamızı da isteyebilirsiniz.

3.10. Rızayı Geri Çekme Hakkı

Kişisel verilerinizin bankamız tarafından işlenmesine ilişkin onayınızı istediğiniz zaman geri çekme hakkına sahipsiniz. Bu, geri çekilmeden önce yaptığımız işlemlerin yasallığını etkilemeyecektir.

Uygulanabilirlik:

Bu hak yalnızca kişisel verilerinizin işlenmesine ilişkin tek yasal dayanağın sizin rızanız olduğu durumlarda geçerlidir.

3.11. Şikayette Bulunma Hakkı

Bankamızın kişisel verilerinizi veri koruma mevzuatına uygun olarak işlemediğini düşünüyorsanız şikayette bulunma hakkınız bulunmaktadır .

Uygulanabilirlik:

Bu hak her zaman geçerlidir.

3.12. Veri Koruma Görevlisi

Bu haklardan herhangi birini kullanmak istiyorsanız lütfen Veri Koruma Görevlisine yazın;

Veri Koruma Görevlisi: Bilge Bank A.Ş.

Adres: Refik Saydam Cad. No:39 Şişhane, Beyoğlu – İstanbul Bilge Bank A.Ş.

Telefon: +90 216 00 00

Fax: +90 216 00 01

Web Adresi: www.bilgebank.com.tr

Kep Adresi: bilgebank@hs01.kep.tr



3.13. Kısıtlamalar

- Veri denetleyicisinin veya işleyicisinin tabi olduğu Birlik veya Üye Devlet hukuku , 12 ila 22. maddeler ve 34. madde ile 5. maddede öngörülen yükümlülüklerin ve hakların kapsamını, mevzuat tedbiri yoluyla kısıtlayabilir. Böyle bir kısıtlamanın temel hak ve özgürlüklerin özüne saygı göstermesi ve demokratik bir toplumda aşağıdakileri korumak için gerekli ve orantılı bir önlem olması durumunda, hükümler 12 ila 22. maddelerde öngörülen hak ve yükümlülüklerle karşılık gelir :
 - o Ulusal Güvenlik;
 - o savunma;
 - o Kamu güvenliği;
 - o kamu güvenliğine yönelik tehditlere karşı koruma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai cezaların infazı;
 - o Birliğin veya bir Üye Devletin genel kamu çıkarını ilgilendiren diğer önemli hedefler, özellikle parasal, bütçesel ve vergisel konular, kamu sağlığı ve sosyal güvenlik dahil olmak üzere Birliğin veya bir Üye Devletin önemli ekonomik veya mali çıkarları;
 - o yargı bağımsızlığının ve yargı işlemlerinin korunması;
 - o düzenlenmiş mesleklere ilişkin etik ihlallerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması;

- o (a) ila (e) ve (g) bentlerinde belirtilen durumlarda, ara sıra da olsa, resmi otoritenin kullanılmasıyla bağlantılı bir izleme, teftiş veya düzenleme işlevi;
 - o veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması;
 - o medeni hukuk iddialarının uygulanması.
- Özellikle, 1. paragrafta atıfta bulunulan herhangi bir yasal tedbir, ilgili olduğu yerde en azından aşağıdakilere ilişkin özel hükümler içerecektir:
 - o işlemin amaçları veya işleme kategorileri;
 - o kişisel veri kategorileri;
 - o getirilen kısıtlamaların kapsamı;
 - o kötüye kullanımı veya yasa dışı erişimi veya aktarımı önleyecek önlemler;
 - o kontrolörün veya kontrolör kategorilerinin spesifikasyonu;
 - o işlemin niteliği, kapsamı ve amaçları veya işleme kategorileri dikkate alınarak saklama süreleri ve geçerli önlemler;
 - o veri sahiplerinin hak ve özgürlüklerine yönelik riskler; Ve
 - o kısıtlamanın amacına zarar vermediği sürece, veri sahiplerinin kısıtlama hakkında bilgilendirilme hakkı.



BÖLÜM 4. KONTROLÖR VE İŞLEYİCİ

4.1. Kontrolörün Sorumluluğu (Madde 24)

1. Kontrolör, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyeyle sahip riskleri dikkate alarak, işleme faaliyetinin bu Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Bu tedbirler gözden geçirilir ve gerektiğinde, güncellenir.
2. İşleme faaliyetleri ile ilgili olarak ölçülü olması halinde, 1. paragrafta atıfta bulunulan tedbirler kontrolör tarafından uygun veri koruma politikalarının uygulanmasını kapsar.
3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmalarına uygun hareket edilmesi kontrolörün yükümlülüklerine uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.

4.2. Özel ve Olağan Veri Koruması (Madde 25)

1. Kontrolör, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyeyle sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, verilerin en alt düzeye indirilmesi gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzük'ün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma ad kullanımı gibi uygun teknik ve düzenlemeye ilişkin tedbirler uygular ve veri sahiplerinin haklarını korur.
2. Kontrolör, olağan durumda, yalnızca her spesifik işleme amacı için gereken kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Söz konusu yükümlülük toplanan kişisel veri miktarı, bunların işlenme derecesi, saklama süresi ve bunlara erişilebilirliğe uygulanır. Özellikle, söz konusu tedbirler, olağan durumda, bireyin müdahalesi olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine açılmamasını sağlar.

3. 42. madde uyarınca onaylı bir belgelendirme mekanizması bu maddenin 1 ve 2. paragraflarında ortaya konan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.

4.2.1 Kişisel Verilerin Korunması

Kişisel verilerinizin korunması ve hukuka aykırı bir şekilde erişimini önlemek için GDPR doğrultusunda bankamız tarafından gerekli idari ve teknik tedbirler alınmakta, Banka içinde prosedürler düzenlenmekte, aydınlatma ve açık rıza metinleri hazırlanmakta ve GDPR hükümlerinin uygulanmasını sağlamak için gerekli denetimler yapılmakta veya dışardan hizmet alımı yoluyla yaptırılmaktadır. Bu denetim sonuçları Bankanın iç işleyişi kapsamında değerlendirilir ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülür.

Yukarıda belirtilen kişisel verileriniz, bankamıza ve/veya tedarikçilerimize ait fiziki arşivler ve bilişim sistemlerine nakledilerek, hem dijital hem de fiziki ortamda muhafaza altında tutulabilecektir. Kişisel verilerin güvenliğini sağlamak için alınan teknik ve idari tedbirler aşağıda iki başlık altında detaylı bir şekilde açıklanmaktadır.

Teknik Tedbirler

- 1) Toplanan kişisel bilgilerin korunması için Secure Socket Layer (SSL) adı verilen standart teknoloji de dahil olmak üzere, genel kabul görmüş standart teknolojileri ve işletme güvenliği yöntemlerini kullanmaktayız. Ancak, İnternet'in özelliği dolayısıyla bilgilere yetkisiz kişiler tarafından ağlar üzerinden gerekli güvenlik önlemleri olmaksızın erişilebilmektedir. Teknolojinin güncel durumuna, teknolojik uygulamanın maliyetine ve korunacak verilerin niteliğine bağlı olarak, verilerinizin imha, kayıp, tahrifat, izinsiz ifşa veya izinsiz erişim gibi risklerden korumak için teknik ve idari tedbirleri almaktayız. Bu kapsamda birlikte çalıştığımız hizmet sağlayıcılarla veri güvenliğine ilişkin sözleşmeler akdetmekteyiz.
- 2) Siber Güvenliğin Sağlanması: Kişisel veri güvenliğinin sağlanması için siber güvenlik ürünleri kullanılmaktayız ancak aldığımız teknik tedbirler bununla sınırlı değildir. Güvenlik duvarı ve ağ geçidi gibi tedbirler ile internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattını oluşturulmaktadır. Bununla birlikte hemen hemen her yazılım ve donanım bir takım kurulum ve yapılandırma işlemlerine tabi tutulmaktadır. Yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları olabileceği dikkate alınarak, kullanılmayan yazılım ve servisler cihazlardan kaldırılmaktadır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilmektedir. Yama yönetimi ve yazılım güncellemeleri ile yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi sağlanmaktadır.

- 3) Eriřim Sınırlamaları: Kiřisel veri ieren sistemlere eriřim yetkileri sınırlandırılmakta ve dzenli olarak gzden geirilmektedir. Bu kapsamda alıřanlara, yapmakta oldukları iř ve grevler ile yetki ve sorumlulukları iin gerekli olduėu lde eriřim yetkisi tanınmakta ve kullanıcı adı ve řifre kullanılmak suretiyle ilgili sistemlere eriřim saėlanmaktadır. Sz konusu řifre ve parolalar oluřturulurken, kiřisel bilgilerle iliřkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine byk kk harf, rakam ve sembollerden oluřacak kombinasyonların tercih edilmesi saėlanmaktadır. Buna baėlı olarak, eriřim yetki ve kontrol matrisi oluřturulmaktadır.
- 4) řifreleme: Gl řifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak iin řifre giriři deneme sayısının sınırlandırılması, dzenli aralıklarla řifre ve parolaların deėiřtirilmesinin saėlanması, ynetici hesabı ve admin yetkisinin sadece ihtiya olduėu durumlarda kullanılması iin aılması ve veri sorumlusuyla iliřikleri kesilen alıřanlar iin zaman kaybetmeksizin hesabın silinmesi ya da giriřlerin kapatılması gibi yntemlerle eriřimin sınırlandırılması yapılmaktadır.

- 5) Anti Virs Yazılımları: Kt amalı yazılımlardan korunmak iin ayrıca, bilgi sistem aėını dzenli olarak tarayan ve tehlikeleri tespit eden antivirs, antispam gibi rnlerin kullanılmakta, ayrıca bunlar gncel tutularak gereken dosyaların dzenli olarak taranmaktadır. Farklı internet siteleri ve/veya mobil uygulama kanallarından kiřisel veri temin edilecekse, baėlantıların SSL ya da daha gvenli bir yol ile gerekleřtirilmesi saėlanmaktadır.

BİLGE BANK A.ř.

- 6) Kiřisel Veri Gvenliėinin Takibi: Biliřim aėlarında hangi yazılım ve servislerin alıřtıėının kontrol edilmesi, Biliřim aėlarında sızma veya olmaması gereken bir hareket olup olmadıėının belirlenmesi, Tm kullanıcıların iřlem hareketleri kaydının dzenli olarak tutulması (log kayıtları gibi), Gvenlik sorunlarının mmkn olduėunca hızlı bir řekilde raporlanması, Yapılmaktadır. Yine alıřanların sistem ve servislerdeki gvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi iin resmi bir raporlama prosedr oluřturulmaktadır. Biliřim sisteminin okmesi, kt niyetli yazılım, servis dıřı bırakma saldırısı, eksik veya hatalı veri giriři, gizlilik ve btnlė bozan ihlaller, biliřim sisteminin ktye kullanılması gibi istenmeyen olaylarda deliller toplanmakta ve gvenli bir řekilde saklanmaktadır.
- 7) Kiřisel Veri İeren Ortamların Gvenliėinin Saėlanması: Kiřisel veriler, veri sorumlularının yerleřkelerinde yer alan cihazlarda ya da kėıt ortamında saklanıyor ise, bu cihazların ve kėıtların alınması veya kaybolması gibi tehditlere karřı fiziksel gvenlik nlemleri alınmaktadır. Kiřisel verilerin yer aldıėı fiziksel ortamların dıř risklere (yangın, sel vb.) karřı uygun yntemlerle korunmakta ve bu ortamlara giriř / ıkıřlar kontrol altına alınmaktadır.

Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlali önlemek için ağ bileşenleri arasında erişim sınırlandırılabilen veya bileşenlerin ayrılması sağlanmaktadır. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilir.

Aynı seviyedeki önlemler Banka yerleşkesi dışında yer alan ve Bankaya ait kişisel veri içeren kâğıt ortamları, elektronik ortam ve cihazlar için de alınmaktadır. Nitekim kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılabilecek kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmektedir. Çalışanların şahsi elektronik cihazları ile bilgi sistem ağına erişim sağlaması durumunda bunlar için de yeterli güvenlik tedbirleri alınmaktadır.

Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması yöntemi uygulanmaktadır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmakta ve yetkisiz erişim önlenmektedir. Kişisel veri içeren kâğıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmakta, söz konusu evraklara yetkisiz erişim önlenmektedir.

BİLGE BANK A.Ş.

Bankamız, GDPR uyarınca kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede DPO ve veri sahiplerine bildirir. DPO , gerekli görmesi halinde bu durumu internet sitesinde veya başka bir yöntemle ilan edebilir.

- 8) Kişisel Verilerin Bulutta Depolanması: Kişisel verilerin bulutta depolanması durumunda, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının Banka tarafından değerlendirilmesi gerekmektedir. Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolü uygulanmaktadır. Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması sağlanmaktadır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyaları yok edilmektedir.

Kişisel verilerin bulunduğu veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri ilgililere anlık olarak iletilmektedir.

9) Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakım: Banka tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmaktadır.

10) Kişisel Verilerin Yedeklenmesi: Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde Banka yedeklenen verileri kullanarak en kısa sürede faaliyete geçmeyi sağlamaktadır. Yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olup, veri seti yedekleri ağ dışında tutulmaktadır.

- Bankamızın yürütmüş olduğu tüm faaliyetler detaylı olarak tüm iş birimleri özelinde analiz edilmiş ve bu analiz neticesinde süreç bazlı bir kişisel veri işleme envanteri hazırlanmıştır. Bu envanterdeki riskli alanlar tespit edilerek gerekli hukuki ve teknik tedbirler sürekli olarak alınmaktadır.
- Bankamız tarafından gerçekleştirilen kişisel veri işleme faaliyetleri bilgi güvenliği sistemleri, teknik sistemlerle ve hukuki yöntemlerle denetlenmektedir. Kişisel veri güvenliğine ilişkin politika ve prosedürler belirlenmekte bu kapsamda düzenli kontroller yapılmaktadır.
- Bankamız, bilgi teknolojileri ihtiyaçlarını karşılayabilmek için zaman zaman harici hizmet sağlayıcı firmalardan hizmet alabilmektedir. Bu durumda söz konusu Veri İşleyen harici hizmet sağlayıcıların en az bankamızın sağladığı güvenlik önlemlerini sağladığından emin olarak işlem yapılmaktadır. Bu durumda, Veri İşleyen ile yazılı bir sözleşme imzalanarak imzalanan bu sözleşmede asgari olarak aşağıdaki hususlara yer verilmektedir:
 - o Veri İşleyen'in sadece Veri Sorumlusu'nun talimatları doğrultusunda sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve GDPR ve sair mevzuata uygun bir şekilde hareket etmesi gerektiği,
 - o GDPR'a uygun bir şekilde hareket etmesi gerektiği,
 - o Veri İşleyen'in işlediği kişisel verilere ilişkin süresiz süresiz sır saklama yükümlülüğüne tabi olduğu,
 - o Herhangi bir veri ihlali olması durumunda Veri İşleyen'in bu durumu derhal Veri Sorumlusu'na bildirmekle yükümlü olduğu,
 - o Bankamızın Veri İşleyen'in kişisel veri içeren sistemleri üzerinde gerekli denetimleri yapacağı veya yaptıracağı, denetim sonucu ortaya çıkan raporları ve hizmet sağlayıcı firmayı yerinde inceleyebileceği,
 - o Veri İşleyen'in kişisel verilerin güvenliği için gerekli teknik ve idari tedbirleri alacağı

Veri İşleyen ile aramızdaki ilişkinin niteliği elverdikçe Veri İşleyen'e aktarılan kişisel verilerin kategori ve türleri de ayrı bir maddede belirtilmektedir.

- Kurum'un rehber ve yayınlarında vurguladığı üzere veri minimizasyonu prensibi çerçevesinde kişisel veriler mümkün olduğunca azaltılmakta ve gerekli olmayan, güncelliğini yitirmiş ve bir amaca hizmet etmeyen kişisel veriler toplanmamakta ve eğer GDPR'dan önceki dönemde toplandıysa Kişisel Veri Saklama ve İmha Politika'sına uygun bir şekilde imha edilmektedir.
- Teknik hususlar konusunda uzman personel istihdam edilmektedir.
- Bankamız çalışanlarının işe alınma süreçlerinde imzalanacak İş Sözleşmelerinde gizliliğe ve veri güvenliğine ilişkin olarak hükümler belirlemiştir ve çalışanlardan bu hükümlere uymasını istemektedir. Çalışanlar, kişisel verilerin korunması hukuku ve bu hukuka uygun olarak gerekli önlemlerin alınması konusunda düzenli olarak bilgilendirilmekte ve eğitilmektedir. Çalışanların rol ve sorumlulukları bu kapsamda gözden geçirilmiş ve görev tanımları revize edilmiştir.
- Teknolojik gelişmelere uygun şekilde teknik önlemler alınmakta, alınan önlemler periyodik olarak kontrol edilmekte, güncellenmekte ve yenilenmektedir.
- Erişim yetkileri sınırlandırılmakta, yetkiler düzenli olarak gözden geçirilmektedir.
- Alınan teknik önlemler düzenli olarak yetkilisine raporlanmakta, risk oluşturan hususlar yeniden gözden geçirilerek gerekli teknolojik çözümlerin üretilmesi için çalışılmaktadır.
- Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.
- Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için yedekleme programları kullanılmaktadır.
- Saklanma alanlarına yönelik güvenlik sistemleri kullanılmakta, alınan teknik önlemler periyodik olarak iç kontroller gereği ilgisine raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözümler üretilmektedir. Fiziksel ortamda saklanan dosyalar/çıktılar çalışılan tedarikçi firmalar aracılığı ile saklanmakta ve sonrasında belirlenen prosedürlere uygun olarak imha edilmektedir.

4.2.2 Özel Nitelikli Kişisel Verilerin Korunması

Özel nitelikli kişisel verilerin işlenmesi ve korunması ile ilgili ayrı bir politika hazırlanmış ve yürürlüğe alınmıştır.

GDPR ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşıdıkları için özel nitelikli kişisel veri olarak düzenlemiş ve bu verilerin işlenmesini daha hassas bir korumaya tabi tutmuştur.

Bankamız, GDPR maddesine uygun olarak, özel nitelikli kişisel verilerin elde edilmesi sırasında İlgili Kişiler'i aydınlatmaktadır. Özel nitelikli kişisel veriler, GDPR'a uygun tedbirler alınarak ve gerekli denetimler yapılarak/yaptırılarak işlenmektedir. Kural olarak özel

nitelikli kişisel verilerin işleme şartlarından bir diğeri ise veri sahibinin açık rızasıdır. Bankamız, veri sahiplerine açık rızalarını belirli bir konuya ilişkin, bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklama fırsatını sunmaktadır.

Bankamız, kural olarak özel nitelikli kişisel verilerin işlenmesi için İlgili Kişiler'in açık rızalarını yazılı olarak almaktadır. Bunun yanında, sağlık ve cinsel hayata ilişkin kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğini düzenlemektedir. Hangi nedene dayanırsa dayansın, işleme süreçlerinde daima genel veri işleme ilkeleri dikkate alınır ve buna ilkelere uygunluk sağlanır.

Bankamız, özel nitelikli kişisel verilerin güvenliğinin sağlanması için özel önlemler almaktadır. Veri minimizasyonu ilkesi gereği, özel nitelikli kişisel veriler, ilgili iş süreci için gerekli olmadığı sürece toplanmamakta ve yalnızca gerekli durumlarda işlenmektedir. Özel nitelikli kişisel veri işlenmesi durumunda kanuni yükümlülüklerle uymak ve DPO tarafından belirlenen önlemlere uyum sağlamak için gerekli görülen teknik ve idari tedbirler alınmaktadır.

4.3. Ortak Kontrolörler (Madde 26)

1. İki ya da daha fazla sayıda kontrolörün işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, bu kontrolörler ortak kontrolörlerdir. Ortak kontrolörler, kontrolörlerin ilgili sorumlulukları kontrolörün tabi olduğu Birlik veya üye devlet hukuku çerçevesinde belirlenmedikçe ve belirlendiği sürece, özellikle veri sahibinin haklarının kullanımı ve 13 ve 14. maddelerde atıfta bulunulan bilgi sağlama görevleri ile ilgili olarak bu Tüzük kapsamındaki yükümlülüklerle uygunluğa ilişkin sorumluluklarını aralarındaki bir düzenleme vasıtasıyla şeffaf bir şekilde belirler. Düzenleme çerçevesinde veri sahiplerine yönelik bir temas noktası belirlenebilir.

2. 1. paragrafta atıfta bulunulan düzenleme ortak kontrolörlerin veri sahipleriyle karşılıklı rolleri ve ilişkilerini uygun şekilde yansıtır. Düzenlemenin mahiyeti veri sahibine sağlanır.

3. 1. paragrafta atıfta bulunulan düzenlemenin koşullarına bakılmaksızın, veri sahibi bu Tüzük kapsamındaki haklarını her kontrolör açısından ve her kontrolöre karşı kullanabilir.

4.4. Birlik İçerisinde Kurulu Olmayan Kontrolörler veya İşleyicilerin Temsilcileri (Madde 27)

1. 3(2) maddesinin uygulandığı hallerde, kontrolör veya işleyici yazılı olarak Birlik içerisinde bir temsilci belirtir.

2. Bu maddenin 1. paragrafında belirtilen yükümlölük aşğıdaki durumlara uygulanmaz: (a) nadiren gerekleşen, 9(1) maddesinde atıfta bulunulan özel veri kategorilerinin işlenmesini büyük aplı olarak içeren işleme faaliyeti veya 10. maddede atıfta bulunulan mahkumiyet kararları ve ceza gerektiren suçlar ile ilgili olan ve, işleme faaliyetinin mahiyeti, bağlamı, kapsamı ve amaçları dikkate alındığında, gerek kişilerin hakları ve özgürlükleri açısından bir riske sebep olması muhtemel olmayan bir işleme faaliyeti veya (b) bir kamu kuruluşu veya organı.
3. Temsilcilik kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen veri sahiplerinin bulunduğu üye devletlerin birinde kurulur.
4. Temsilci, işleme faaliyeti ile ilgili tüm hususlarda, bu Tüzük'e uygunluk sağlanması amacıyla, özellikle denetim makamları ve veri sahipleri tarafından kontrolör veya işleyiciye ek olarak veya bunlar yerine muhatap kabul edilmek üzere kontrolör veya işleyici tarafından yetkilendirilir.
5. Kontrolör veya işleyici tarafından bir temsilci belirlenmesiyle kontrolör veya işleyiciye karşı açılacak davalara hanel gelmez.

4.5. İşleyici (Madde 28)

1. Bir kontrolör adına bir işleme faaliyetinin gerekleştirilmesinin gerektiği hallerde, kontrolör ancak işleme faaliyetinin bu Tüzük'ün gerekliliklerinin yerine getirilmesini ve veri sahibinin haklarının korunmasını sağlayacak biçimde uygun teknik ve düzenlemeye ilişkin tedbirler uygulama hususunda yeterli güvenceler sağlayan işleyiciler kullanır.
2. İşleyici kontrolörün önceden verdiği spesifik veya genel yazılı onay olmaksızın başka bir işleyiciyle çalışamaz. Genel yazılı onay halinde, işleyici diğer işleyicilerin eklenmesi veya değiştirilmesi ile ilgili planlanan değişiklikler hususunda kontrolörü bilgilendirerek kontrolöre söz konusu değişikliklere itiraz etme olanağı tanır. 3. Bir işleyici tarafından işleme faaliyeti gerekleştirilmesi Birlik veya üye devlet hukuku çerçevesinde düzenlenen, kontrolör ile ilgili olarak işleyici açısından bağlayıcı olan ve işleme faaliyetinin konusu ve süresi, işleme faaliyetinin mahiyeti ve amacı, kişisel verilerin türü ve veri sahiplerinin kategorileri ile kontrolörün yükümlölükleri ve haklarının ortaya konduğu bir sözleşme veya diğer hukuki tasarruflar ile düzenlenir. Söz konusu sözleşme veya diğer hukuki tasarruflarda özellikle işleyicinin şunları yapacağı belirtilir:
 - (a) işleyicinin tabi olduğu Birlik veya üye devlet hukuku çerçevesinde bu yönde bir gereklilik bulunmaması halinde, üçüncü bir ülkeye veya uluslararası bir kuruluşa kişisel veri aktarımları ile ilgili olanlar da dahil olmak üzere yalnızca kontrolörün verdiği belgelendirilmiş talimatlar doğrultusunda kişisel verilerin işlenmesi; bu durumda, kanunlar çerçevesinde söz konusu bilgilendirmenin önemli kamu yararı gerekçeleriyle yasaklanmaması halinde, işleyici kontrolörü işleme faaliyetinden önce bu yasal gereksinimden haberdar eder;
 - (b) kişisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüdünde bulunmasının veya uygun bir yasal gizlilik yükümlölüğü altında bulunmasının sağlanması;
 - (c) 32. madde uyarınca gerekli tüm tedbirlerin alınması;

(d) başka bir işleyiciyle çalışılması amacıyla 2 ve 4. paragraflarda atıfta bulunulan koşullara riayet edilmesi;

(e) işleme faaliyetinin mahiyetinin dikkate alınması suretiyle, kontrolörün veri sahibinin Bölüm III'te belirtilen haklarının kullanımına ilişkin taleplere yanıt verme yükümlülüğünün yerine getirilmesine yönelik olarak, uygun teknik ve düzenlemeye ilişkin tedbirler vasıtasıyla, kontrolöre mümkün olduğunca yardımcı olunması;

(f) işleme faaliyetinin mahiyeti ve işleyiciye sağlanan bilgilerin dikkate alınması suretiyle, 32 ila 36. maddeler uyarınca yükümlülüklerle uygun hareket edilmesinin sağlanmasında kontrolöre yardımcı olunması;

(g) kontrolörün tercihi üzerine, işleme faaliyeti ile ilgili hizmetlerin sağlanmasından sonra tüm kişisel verilerin silinmesi veya kontrolöre iade edilmesi ve, Birlik ya da üye devlet hukuku çerçevesinde kişisel verilerin saklanmasıyla ilgili gerekli olmaması durumunda, mevcut nüshaların silinmesi;

(h) bu maddede ortaya konan yükümlülüklerle uygunluğun gösterilmesi için gereken tüm bilgilerin kontrolöre sağlanması ve teftişler de dahil olmak üzere kontrolör tarafından ya da kontrolörce yetkilendirilen başka bir denetçi tarafından gerçekleştirilen denetimlere izin verilmesi ve katkıda bulunulması.

İlk alt paragrafın (h) bendi ile ilgili olarak, kendi görüşüne göre bir talimatın bu Tüzük veya Birlik ya da üye devletin diğer veri koruma hükümlerini ihlal etmesi durumunda, kontrolörü ivedilikle bilgilendirir.

4. Bir işleyicinin kontrolör adına spesifik işleme faaliyetlerinin gerçekleştirilmesine yönelik olarak başka bir işleyici ile çalıştığı durumlarda, 3. paragrafta atıfta bulunulduğu üzere kontrolör ve işleyici arasındaki sözleşme veya başka bir hukuki tasarrufla ortaya konan veri koruma yükümlülükleri özellikle işleme faaliyetinin bu Tüzük'ün gerekliliklerinin yerine getirilmesini sağlayacak şekilde uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanması amacı ile yeterli teminatlar sağlayan bir sözleşme ya da Birlik veya üye devlet hukuku kapsamındaki başka bir hukuki tasarruf yoluyla diğer işleyici açısından da uygulanır. Diğer işleyicinin veri koruma yükümlülüklerini yerine getiremediği hallerde, ilk işleyici diğer işleyicinin yükümlülüklerinin ifası konusunda kontrolöre karşı tam yükümlülük sahibi olmaya devam eder.

5. Bir işleyicinin 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmalarına uygun hareket etmesi bu maddenin 1 ve 4. paragraflarında atıfta bulunulan yeterli teminatların gösterilmesine ilişkin bir unsur olarak kullanılabilir.

6. Kontrolör ve işleyici arasındaki bireysel bir sözleşmeye hâle gelmeksizin, bu maddenin 3 ve 4. paragraflarında atıfta bulunulan sözleşme ya da başka bir hukuki tasarruf, 42 ve 43. maddeler uyarınca kontrolör veya işleyiciye sağlanan bir belgelendirmenin parçası olmaları durumu da dahil olmak üzere, tamamen veya kısmen, bu maddenin 7 ve 8. paragraflarında atıfta bulunulan standart sözleşme maddelerine dayanabilir.

7. Komisyon bu maddenin 3 ve 4. paragraflarında atıfta bulunulan hususlara yönelik olarak ve 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca standart sözleşme maddeleri oluşturabilir.

8. Bir denetim makamı bu maddenin 3 ve 4. paragraflarında atıfta bulunulan hususlara yönelik olarak ve 63. maddede atıfta bulunulan tutarlık mekanizması uyarınca standart sözleşme maddeleri kabul edebilir.

9. 3 ve 4. paragraflarda atıfta bulunulan sözleşme veya diğer hukuki tasarruflar elektronik format da dahil olmak üzere yazılı olarak hazırlanır.

10. 82, 83 ve 84. maddelere hâle gelmeksizin, bir işleyicinin işleme amaçları ve yöntemlerini belirleyerek bu Tüzük'ü ihlal etmesi durumunda, işleyici bu işleme faaliyeti açısından bir kontrolör olarak değerlendirilir.

4.6. Kontrolör veya İşleyicinin Yetkisi Kapsamındaki İşleme Faaliyet (Madde 29)

İşleyici ve kontrolör ya da işleyicinin yetkisi ile hareket eden ve kişisel verilere erişimi bulunan herhangi bir kişi, Birlik ya da üye devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, kontrolörden aldığı talimatlar haricinde bu verileri işleyemez.

4.7. İşleme Faaliyetlerinin Kayıtları (Madde 30)

1. Her kontrolör ve, uygun olduğu hallerde, kontrolörün temsilcisi kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutar. Bu kayıt aşağıdaki bilgilerin tamamını ihtiva eder:

(a) kontrolör ve, uygun olduğu hallerde, ortak kontrolör, kontrolörün temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) işleme amaçları;

(c) veri sahibi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama;

(d) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri;

(e) uygun olduğu hallerde, üçüncü bir ülke veya uluslararası bir kuruluşun tanımlanması ve, 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun güvencelere ilişkin belgelendirme de dahil olmak üzere, söz konusu üçüncü ülke veya uluslararası kuruluşla yönelik kişisel veri aktarımları;

(f) mümkün olması halinde, farklı kategorilerdeki verilerin silinmesiyle ilgili öngörülen süre sınırları;

(g) mümkün olması halinde, 32(1) maddesinde atıfta bulunulan teknik ve düzenlemeye ilişkin güvenlik tedbirlerine yönelik genel bir açıklama.

2. Her işleyici ve, uygun olduğu hallerde, işleyicinin temsilcisi bir kontrolör adına gerçekleştirilen tüm kategorilerdeki işleme faaliyetlerine ilişkin olarak aşağıdakileri ihtiva eden bir kayıt tutar:

(a) işleyici veya işleyiciler ile işleyicinin adına hareket ettiği her kontrolörün ve, uygun olduğu hallerde, kontrolör ya da işleyicinin temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) her işleyici adına gerçekleştirilen işleme kategorileri;

(c) uygun olduğu hallerde, üçüncü bir ülke veya uluslararası bir kuruluşun tanımlanması ve, 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun güvencelere ilişkin belgelendirme de dahil olmak üzere, söz konusu üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları;

(d) mümkün olması halinde, 32(1) maddesinde atıfta bulunulan teknik ve düzenlemeye ilişkin güvenlik tedbirlerine yönelik genel bir açıklama.

3. 1 ve 2. paragraflarda atıfta bulunulan kayıtlar elektronik format da dahil olmak üzere yazılı olarak tutulur.

4. Kontrolör ve işleyici ile, uygun olduğu hallerde, kontrolörün veya işleyicinin temsilcisi, talep üzerine, kayıtları denetim makamına sağlar.

5. Gerçekleştirdiği işleme faaliyetinin veri sahiplerinin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması, işleme faaliyetinin nadiren gerçekleştirilmemesi veya işleme faaliyetinin 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verileri yad a 10. maddede atıfta bulunulan mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verileri kapsamaması durumunda, 1 ve 2. paragraflarda atıfta bulunulan yükümlülükler 250'den az kişi istihdam eden bir işletme veya kuruluşa uygulanmaz.

4.8. Denetim Makamıyla İşbirliği (Madde 31)

Kontrolör ve işleyici ile, uygun olduğu hallerde, bunların temsilcileri, talep üzerine, görevlerinin yürütülmesi ile ilgili olarak denetim makamı ile işbirliği yapar.

4.9. İşleme Güvenliği (Madde 32)

1. Kontrolör ve işleyici, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir

güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, aşağıdakiler de dahil olmak üzere uygun teknik ve düzenlemeye ilişkin tedbirler uygulanır:

- (a) kişisel verilerde takma ad kullanımı ve şifreleme;
- (b) işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi;
- (c) fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi;
- (d) işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç.

2. Uygun güvenlik seviyesi değerlendirilirken, iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı olarak imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişim başta olmak üzere özellikle işleme faaliyetinin yol açtığı riskler göz önünde bulundurulur.

3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmasına uygun hareket edilmesi bu maddenin 1. paragrafında ortaya konan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.

4. Kontrolör ve işleyici kontrolör ya da işleyicinin yetkisi ile hareket eden ve kişisel verilere erişimi bulunan herhangi bir gerçek kişinin, Birlik ya da üye devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, kontrolörden aldığı talimatlar haricinde bu verileri işlememesini sağlamak üzere adımlar atar.

4.10. Bir Kişisel Veri İhlalinin Denetim Makamına Bildirilmesi (Madde 33)

1. Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, kontrolör, gereksiz gecikmeye mahal vermeden ve, uygun olması halinde, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde, kişisel veri ihlalinin 55. madde uyarınca yetkin denetim makamına bildirir.

Denetim makamına yönelik bildirimin 72 saat içerisinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir.

2. İşleyici, bir kişisel veri ihlalden haberdar olduktan sonra, herhangi bir gecikmeye mahal vermeden, kontrolöre bildirimde bulunur. 3. 1. paragrafta atıfta bulunulan bildirimde en azından:

- (a) uygun olduğu hallerde, ilgili veri sahibi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dahil olmak üzere kişisel veri ihlalinin mahiyeti açıklanır;
- (b) veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgileri iletilir;

(c) kişisel veri ihlalinin olası sonuçları açıklanır;

(d) uygun olduğu hallerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dahil olmak üzere kişisel veri ihlalinin ele alınması için kontrolör tarafından alınan veya alınması önerilen tedbirler açıklanır.

4. Bilgilerin aynı zamanda sağlanmasının mümkün olmadığı hallerde ve ölçüde, bilgiler gereksiz herhangi bir ek gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir.

5. Kontrolör kişisel veri ihlallerini kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. Bu belgelendirme denetim makamının bu maddeye uyumluluğu doğrulamasını sağlar.

4.11. Bir Kişisel Veri İhlalinin Veri Sahibine İletilmesi (Madde 34)

1. Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör kişisel veri ihlalinin gereksiz bir gecikmeye mahal vermeden veri sahibine iletir.

2. Bu maddenin 1. paragrafında atıfta bulunulan veri sahibine ilişkin bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanır ve en azından 33(3) maddesinin (b), (c) ve (d) bentlerinde atıfta bulunulan bilgiler ve tedbirlere yer verilir.

3. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda, 1. paragrafta atıfta bulunulan veri sahibine ilişkin bildirim gerekmez:

(a) kontrolörün uygun teknik ve düzenlemeye ilişkin koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalinin etkilenen kişisel verilere uygulanmış olması;

(b) kontrolörün 1. paragrafta atıfta bulunulan veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması;

(c) bildirimin ölçüsüz bir çaba gerektirecek olması. Bu durumda, bunun yerine, veri sahiplerinin aynı etkililikle bilgilendirildiği kamuya yönelik bir bildirim veya benzeri bir tedbir uygulanır.

4. Kontrolörün halihazırda kişisel veri ihlalinin veri sahibine iletmemiş olması durumunda, denetim makamı, kişisel veri ihlalinin yüksek bir riske sebebiyet verme olasılığını değerlendirdikten sonra, kontrolörün bu bildirimi yapmasını şart koşabilir veya 3. paragrafta atıfta bulunulan koşullardan herhangi birinin yerine getirilmesine karar verebilir.

4.12. Veri Koruma Etki Değerlendirmesi (Madde 35)

1. Özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar. Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyeti ele alınabilir.

2. Kontrolör, bir veri koruma etki değerlendirmesi gerçekleştirirken, belirlenmiş olması halinde, veri koruma görevlisinin tavsiyesine başvurur.

3. 1. paragrafta atıfta bulunulan bir veri koruma etki değerlendirmesine aşağıdaki durumlarda özellikle ihtiyaç duyulur:

(a) gerçek kişilerle ilgili kişisel özellikler hususunda profil çıkarma da dahil olmak üzere otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirme;

(b) 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verilerin veya 10. maddede atıfta bulunulan mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya

(c) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi.

4. Denetim makamı 1. paragraf uyarınca bir veri koruma etki değerlendirmesi gerekliliğine tabi olan işleme faaliyeti türlerine ilişkin bir liste oluşturur ve bu listeyi kamuya açıklar. Denetim makamı bu listeleri 68. maddede atıfta bulunulan Kurula iletir.

5. Denetim makamı herhangi bir veri koruma etki değerlendirmesinin gerekli olmadığı işleme faaliyeti türlerine ilişkin bir liste oluşturur ve bu listeyi kamuya açıklar. Denetim makamı bu listeleri Kurula iletir.

6. 4 ve 5. paragraflarda atıfta bulunulan listelerin kabulünden önce, söz konusu listelerin veri sahiplerine mallar veya hizmetlerin sağlanması ya da onların çeşitli üye devletlerdeki davranışlarının izlenmesi ile ilgili olan veya kişisel verilerin Birlik içerisinde serbest dolaşımını kayda değer ölçüde etkileyebilecek işleme faaliyetlerine yer verildiği hallerde, yetkin denetim makamı 63. maddede atıfta bulunulan tutarlılık mekanizmasını uygular.

7. Değerlendirme en azından şunları içerir: (a) uygun olduğu hallerde, kontrolör tarafından gözetilen meşru menfaat de dahil olmak üzere öngörülen işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik bir açıklama;

(b) işleme faaliyetlerinin amaçlarla ilişkili olarak gerekliliği ve orantılılığına yönelik bir değerlendirme;

(c) 1. paragrafta atıfta bulunulduğu üzere veri sahiplerinin hakları ve özgürlüklerine yönelik risklere ilişkin bir değerlendirme ve

(d) veri sahipleri ve ilgili diğer kişilerin hakları ve meşru menfaatleri dikkate alınarak, kişisel verilerin korunmasının sağlanması ve bu Tüzük'e uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler.

8. 40. maddede atıfta bulunulan onaylı davranış kurallarına ilgili kontrolörler veya işleyiciler tarafından uyum, söz konusu kontrolörler veya işleyiciler tarafından özellikle bir veri koruma etki değerlendirmesi amaçlarına yönelik olarak gerçekleştirilen işleme faaliyetlerinin etkisinin değerlendirilmesi hususunda dikkate alınır.

9. Uygun olduğu hallerde, kontrolör, ticari menfaatler veya kamu menfaatlerinin korunmasına ya da işleme faaliyetlerinin güvenliğine hâlel gelmeksizin, veri sahipleri veya temsilcilerinin amaçlanan işleme faaliyetine ilişkin görüşlerini alır.

10. 6(1) maddesinin (c) veya (e) bendi uyarınca gerçekleştirilen bir işleme faaliyetinin Birlik hukukunda veya kontrolörün tabi olduğu üye devletin kanununda bir yasal dayanağının bulunduğu, söz konusu kanunun spesifik bir işleme faaliyeti veya bir dizi faaliyeti düzenlediği ve bir veri koruma etki değerlendirmesinin söz konusu yasal dayanağın kabulü bağlamında genel bir etki değerlendirmesinin parçası olarak halihazırda gerçekleştirilmiş olduğu hallerde, üye devletlerin işleme faaliyetlerinden önce böylesi bir değerlendirme yapılmasını gerekli görmemesi durumunda, 1 ila 7. paragraflar uygulanmaz.

11. Gerekmesi halinde, en azından işleme faaliyetlerinin teşkil ettiği risk açısından bir değişiklik meydana geldiğinde, kontrolör işleme faaliyetinin veri koruma etki değerlendirmesi uyarınca gerçekleştirilip gerçekleştirilmediğini değerlendirmek üzere bir gözden geçirme gerçekleştirir.

4.13. Ön İstişare (Madde 36)

1. 35. madde kapsamındaki bir veri koruma etki değerlendirmesi sonucunda kontrolör tarafından riskin azaltılması hususunda alınan tedbirlerin olmaması durumunda işleme faaliyetinin yüksek bir riske sebebiyet vereceğinin görüldüğü hallerde, kontrolör işleme faaliyetinden önce denetim makamına danışır.

2. Kontrolörün riski yeterli şekilde tanımlamadığı veya azaltmadığı haller başta olmak üzere denetim makamının 1. paragrafta atıfta bulunulan amaçlanan işleme faaliyetinin bu Tüzük'ü ihlal edeceğini düşündüğü hallerde, denetim makamı, istişare talebinin alınmasından itibaren sekiz haftalık bir süre içerisinde, kontrolöre ve uygun olduğu hallerde işleyiciye, yazılı tavsiyede bulunur ve, 58. maddede atıfta bulunulan yetkilerinden herhangi birini kullanabilir. Bu süre, amaçlanan işleme faaliyetinin karmaşıklığı dikkate alınarak, altı hafta daha uzatılabilir. Denetim makamı, gecikme sebepleri ile birlikte istişare talebinin alınmasından itibaren bir ay içerisinde herhangi bir süre uzatımı ile ilgili olarak kontrolörü ve, uygun olduğu hallerde, işleyiciyi bilgilendirir. Bu süreler, denetim makamı istişare amacıyla talep etmiş olduğu bilgileri elde edene kadar askıya alınabilir.

3. 1. paragraf uyarınca denetim makamına danışılırken, kontrolör denetim makamına şunları sağlar:

(a) uygun olduđu hallerde, kontrolör, ortak kontrolörler ve işleme faaliyetine müdahil işleyicilerin özellikle bir teşebbüsler grubu dahilindeki işleme faaliyetine yönelik sorumlulukları;

(b) planlanan işleme amaçları ve yöntemleri;

(c) veri sahiplerinin hakları ve özgürlüklerinin korunması amacı ile bu Tüzük uyarınca sağlanan tedbirler ve güvenceler;

(d) uygun olduđu hallerde, veri koruma görevlisinin irtibat bilgileri;

(e) 35. maddede belirtilen veri koruma etki değerlendirmesi ve

(f) denetim makamının talep ettiđi diğer bilgiler.

4. Üye devletler bir ulusal parlamento tarafından kabul edilecek bir yasama tedbiri teklifinin veya böylesi bir yasama tedbirine yönelik olarak işleme faaliyetine ilişkin bir düzenleme tedbirinin hazırlanması esnasında denetim makamına danışır.

5. 1. paragrafa bakılmaksızın, üye devlet hukuku çerçevesinde sosyal koruma ve halk sağlığına ilişkin bir işleme faaliyeti de dahil olmak üzere kontrolör tarafından kamu yararına gerçekleştirilen bir görevin yürütülmesine yönelik olarak bir kontrol tarafından gerçekleştirilecek işleme faaliyeti ile alakalı olarak kontrolörlerin denetim makamına danışması ve ön onay alması gerekebilir.

4.14. Veri Koruma Görevlisinin Belirlenmesi (Madde 37)

1. Kontrolör ve işleyici aşağıdaki durumlarda her halükarda bir veri koruma görevlisi belirler:

(a) işleme faaliyetinin kendi yargı yetkisi çerçevesinde hareket eden mahkemeler haricindeki bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi;

(b) kontrolör veya işleyicinin temel faaliyetlerinin yapıları, kapsamaları ve/veya amaçları geređi veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya

(c) kontrolör veya işleyicinin temel faaliyetlerinin 9 maddesi uyarınca özel kategorilerdeki verilerin ve 10. maddede atıfta bulunulan mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi.

4. 1. paragrafta atıfta bulunulanlar haricindeki durumlarda, kontrolör veya işleyici ya da birlikler ve kontrolör ya da işleyici kategorilerini temsil eden diğer organlar bir veri koruma görevlisi belirleyebilir veya Birlik veya üye devlet hukuku çerçevesinde gerektiđi hallerde, bir veri koruma görevlisi belirler. Veri koruma görevlisi söz konusu birlikler ve kontrolörler ya da işleyicileri temsil eden diğer organlar adına hareket edebilir.

5. Veri koruma görevlisi mesleki nitelikler ve özellikle, veri koruma hukuku ve uygulamalarına ilişkin uzmanlık bilgisi ve 39. maddede atıfta bulunulan görevleri yerine getirme kabiliyetine dayalı olarak belirlenir.

6. Veri koruma görevlisi kontrolör veya işleyicinin bir çalışanı olabilir veya görevlerini bir hizmet sözleşmesine dayalı olarak yerine getirebilir.
7. Kontrolör veya işleyici veri koruma görevlisinin irtibat bilgilerini yayımlar ve denetim makamına iletir.

4.15. Veri Koruma Görevlisinin Konumu (Madde 38)

1. Kontrolör ve işleyici veri koruma görevlisinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlar.
2. Kontrolör ve işleyici 39. maddede atıfta bulunulan görevlerin gerçekleştirilmesi, kişisel veriler ile işleme faaliyetlerine erişilmesi ve uzmanlık bilgisinin aynı seviyede tutulması için gereken kaynakları sağlayarak bu görevlerin yerine getirilmesi hususunda veri koruma görevlisine destek verir.
3. Kontrolör ve işleyici veri koruma görevlisinin bu görevlerin yerine getirilmesi ile ilgili olarak hiçbir talimat almamasını sağlar. Veri koruma görevlisi görevlerinin yerine getirilmesi nedeniyle kontrolör ya da işleyici tarafından işten çıkarılamaz veya cezalandırılmaz. Veri koruma görevlisi doğrudan kontrolör veya işleyicinin en üst yönetimine rapor verir.
4. Veri sahipleri kişisel verilerinin işlenmesi ve bu Tüzük kapsamındaki haklarının kullanımı ile ilgili tüm hususlarla alakalı olarak veri koruma görevlisiyle irtibata geçebilir.
5. Veri koruma görevlisi, Birlik veya üye devlet hukuku uyarınca, görevlerinin yerine getirilmesi ile ilgili olarak sır saklama veya gizlilik ilkelerine bağlıdır.
6. Veri koruma görevlisi başka görevleri ve vazifeleri de yerine getirebilir. Kontrolör veya işleyici söz konusu görev ve vazifelerin bir çıkar çatışmasına neden olmamasını sağlar.

Veri koruma yükümlülüklerimiz hakkında bize tavsiyelerde bulunmak ve uyumluluğu izlemek için bir Veri Koruma Görevlisi atadık. Veri Koruma Görevlisine aşağıdaki adrese yazarak ulaşabilirsiniz:

Veri Koruma Görevlisi: Bilge Bank A.Ş.

Adres: Refik Saydam Cad. No:39 Şişhane, Beyoğlu – İstanbul Bilge Bank A.Ş.

Telefon: +90 216 00 00

Fax: +90 216 00 01

Web Adresi: www.bilgebank.com.tr

Kep Adresi: bilgebank@hs01.kep.tr

4.16. Veri Koruma Görevlisinin Görevleri (Madde 39)

1. Veri koruma görevlisinin en azından aşağıdaki görevleri bulunur:

(a) kontrolör veya işleyici ile işleme faaliyetleri gerçekleştiren çalışanların bu Tüzük ile Birlik veya üye devletlerin diğer veri koruma hükümleri uyarınca yükümlülükleri hususunda bilgilendirilmesi ve onlara tavsiyede bulunulması;

(b) bu Tüzük'e, Birlik veya üye devletlerin diğer veri koruma hükümlerine uyumluluğu ve sorumlulukların verilmesi, işleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ve ilgili denetimler de dahil olmak üzere kontrolör veya işleyicinin kişisel verilerin korunmasına ilişkin politikalarına uyumluluğun izlenmesi;

(c) talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunulması ve 35. madde uyarınca bu değerlendirmenin performansının izlenmesi; (d) denetim makamıyla işbirliği yapılması;

(e) 36. maddede atıfta bulunulan ön istişare de dahil olmak üzere işleme faaliyetine ilişkin konularda denetim makamına yönelik bir temas noktası olarak hareket edilmesi ve, uygun olduğu hallerde, diğer her türlü konu ile ilgili olarak danışılması.

2. Veri koruma görevlisi, görevlerini yerine getirirken, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarını dikkate alarak, işleme faaliyetleri ile ilişkili riski göz önünde bulundurur.

4.17. Davranış Kuralları (Madde 40)

1. Üye devletler, denetim makamları, Kurul ve Komisyon, çeşitli işleme sektörlerinin spesifik özellikleri ve mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçlarını dikkate alarak, bu Tüzük'ün düzgün bir şekilde uygulanmasına katkıda bulunması amaçlanan davranış kurallarının hazırlanmasını teşvik eder.

2. Birlikler ve kontrolör veya işleyici kategorilerini temsil eden diğer organlar bu Tüzük'ün aşağıdaki hususlarla alakalı olarak uygulanmasını belirlemek amacıyla davranış kuralları hazırlayabilir veya bu kuralları değiştirebilir ya da bunların kapsamını genişletebilir:

(a) adil ve şeffaf veri işleme;

(b) kontrolörler tarafından spesifik bağlamlarda gözetilen meşru menfaatler;

(c) kişisel verilerin toplanması;

(d) kişisel verilerde takma ad kullanımı;

(e) kamuoyuna ve veri sahiplerine sağlanan bilgiler;

(f) veri sahiplerinin haklarının kullanımı;

(g) çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli;

(h) 24 ve 25. maddelerde atıfta bulunulan tedbirler ve usuller ile 32. maddede atıfta bulunulduğu üzere işleme faaliyetinin güvenliğini sağlanmasına yönelik tedbirler.

(i) kişisel veri ihlallerinin denetim makamlarına bildirim ve söz konusu kişisel veri ihlallerinin veri sahiplerine iletilmesi;

(j) üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarılması veya

(k) veri sahiplerinin 77. ve 79. maddeler uyarınca haklarına hâle gelmeksizin, kontrolörler ve veri sahipleri arasında ihtilafların çözümüyle ilgili mahkeme dışı işlemler ve diğer ihtilaf çözüm usulleri.

3. Bu Tüzük'e tabi kontrolörler veya işleyicilerin uygun hareket etmesine ek olarak, bu maddenin 5. paragrafı uyarınca onaylanan davranış kuralları ve bu maddenin 9. paragrafı uyarınca genel geçerliliğe sahip olunması hususuna 3. madde uyarınca bu Tüzük'e tabi olmayan kontroller veya işleyiciler tarafından da 46(2) maddesinin (e) bendinde atıfta bulunulan koşullar uyarınca üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları çerçevesinde uygun güvenceler sağlanması amacı ile uyulabilir. Söz konusu kontrolörler veya işleyiciler, veri sahiplerinin hakları ile ilgili olanlar da dahil olmak üzere uygun güvenceleri uygulamak üzere sözleşmeye bağlı veya diğer bağlayıcı belgeler vasıtasıyla bağlayıcı ve uygulanabilir taahhütlerde bulunur.

4. Bu maddenin 2. paragrafında atıfta bulunulan davranış kurallarında 41(1) maddesinde atıfta bulunulan organın, 55 veya 56. madde uyarınca yetkin denetim makamlarının görevleri ve yetkilerine hâle gelmeksizin, davranış kurallarını uygulamayı taahhüt eden kontrolörler veya işleyicilerin söz konusu hükümlere uyumluluğunu zorunlu olarak izlemesini sağlayan mekanizmalara yer verilir.

5. Bu maddenin 2. paragrafında atıfta bulunulan ve davranış kuralları hazırlamayı veya mevcut kuralları değiştirmeyi veya mevcut kuralların kapsamını genişletmeyi amaçlayan birlikler ve diğer organlar kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağı 55. madde uyarınca yetkin denetim makamına ibraz eder. Denetim makamı kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağın bu Tüzük'le uyumlu olup olmadığı konusunda bir görüş sunar ve, yeteri kadar uygun güvenceleri sağladığını tespit etmesi durumunda, kurallar, değişiklik veya kapsam genişletmeye ilişkin söz konusu taslağı onaylar.

6. Kurallar veya değişiklik ya da kapsam genişletmeye ilişkin taslağın 5. paragraf uyarınca onaylandığı hallerde ve ilgili davranış kurallarının çeşitli üye devletlerdeki işleme faaliyetleri ile ilgili olmadığı hallerde, denetim makamı kuralları tescil eder ve yayımlar.

7. Davranış kurallarına ilişkin bir taslağın çeşitli üye devletlerdeki işleme faaliyetleri ile ilgili olduğu hallerde, 55. madde uyarınca yetkin olan denetim makamı, kurallar, değişiklik ya da kapsam genişletmeye ilişkin taslağı onaylamadan önce, kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağın bu Tüzük'le uyumlu olup olmadığına veya, bu maddenin 3. paragrafında atıfta bulunulan durumda, uygun güvenceler sağlayıp sağlamadığına ilişkin bir

görüş bildirecek söz konusu taslağı Kurul'a 63. maddede atıfta bulunulan usul çerçevesinde ibraz eder.

8. 7. paragrafta atıfta bulunulan görüşün değişiklik veya kapsam genişletmeye ilişkin taslağın bu Tüzük'le uyumlu olduğu veya, 3. paragrafta atıfta bulunulan durumda, uygun güvenceler sağladığını teyit ettiği hallerde, Kurul görüşünü Komisyon'a sunar.

9. Komisyon, uygulama tasarrufları vasıtasıyla, bu maddenin 8. paragrafı uyarınca kendisine ibraz edilen onaylı davranış kuralları, değişiklik veya kapsam genişletmenin Birlik içerisinde genel geçerliliğe sahip olduğuna karar verebilir. Bu uygulama tasarrufları 93(2) maddesinde belirtilen inceleme usulü uyarınca kabul edilir.

10. Komisyon 9. paragraf uyarınca genel geçerliliğe sahip olduğuna karar verilen onaylı kuralların uygun şekilde ilan edilmesini sağlar.

11. Kurul onaylı tüm davranış kuralları, değişiklikler ve kapsam genişletmelerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar.

4.18. Onaylı Davranış Kurallarının İzlenmesi (Madde 41)

1. Yetkin denetim makamının 57 ve 58. maddeler kapsamındaki görevleri ve yetkilerine halel gelmeksizin, 40. madde uyarınca davranış kurallarına uyumluluk kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan ve bu amaca yönelik olarak yetkin denetim makamı tarafından akredite edilen bir organ tarafından izlenebilir.

2. 1. paragrafta atıfta bulunulan bir organ, aşağıdaki özellikleri taşıması halinde, davranış kurallarına uyumluluğun izlenmesi amacı ile akredite edilebilir:

(a) kuralların konusuna ilişkin bağımsızlığı ve uzmanlığını yetkin denetim makamını tatmin edecek şekilde göstermiş olması;

(b) ilgili kontrolörler ve işleyicilerin kuralları uygulamaya, bunların kuralların hükümlerine uyumluluğunu izlemeye ve uygulamasını düzenli olarak gözden geçirmeye uygunluğunu değerlendirmesini sağlayan usuller oluşturmuş olması;

(c) kurallara veya kuralların bir kontrolör ya da işleyici tarafından uygulanmış olma veya uygulanma şekline ilişkin ihlallere yönelik şikayetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olması ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olması ve

(d) görev ve vazifelerinin bir çıkar çatışmasına neden olmadığını yetkin denetim makamını tatmin edecek şekilde göstermiş olması.

3. Yetkin denetim makamı bu maddenin 1. paragrafında atıfta bulunulan bir organın akreditasyonuna ilişkin taslak kriterleri 63. maddede atıfta bulunulan tutarlık mekanizması uyarınca Kurul'a ibraz eder.

4. Yetkin denetim makamının görevleri ve yetkilerine ve Bölüm VIII'in hükümlerine hâlel gelmeksizin, bu maddenin 1. paragrafında atıfta bulunulan bir organ, kuralların bir kontrolör veya işleyici tarafından ihlali halinde, uygun güvencelere tabi olarak, ilgili kontrolör veya işleyicinin kurallardan askıya alınması veya çıkarılması da dahil olmak üzere uygun işlemleri gerçekleştirir. Söz konusu organ böylesi işlemler ve bu işlemlerin gerçekleştirilme sebepleri hususunda yetkin denetim makamını bilgilendirir.

5. Akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya organ tarafından gerçekleştirilen eylemlerin bu Tüzük'ü ihlal ettiği hallerde, yetkin denetim makamı 1. paragrafta atıfta bulunulan bir organın akreditasyonunu kaldırır.

6. Bu madde kamu kuruluşları ve organları tarafından gerçekleştirilen işleme faaliyetlerine uygulanmaz.

4.19. Belgelendirme (Madde 23)

1. Üye devletler, denetim makamları, Kurul ve Komisyon, kontrolörler ve işleyiciler tarafından gerçekleştirilen işleme faaliyetlerinin bu Tüzük'le uyumluluğunun gösterilmesi amacıyla, özellikle Birlik düzeyinde, veri koruma belgelendirme mekanizmaları ve veri koruma mühürleri ve işaretlerinin oluşturulmasını teşvik eder. Mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçları dikkate alınır.

2. Bu Tüzük'e tabi kontrolörler veya işleyicilerin uygun hareket etmesine ek olarak, bu maddenin 5. paragrafı uyarınca onaylanan veri koruma belgelendirme mekanizmaları, mühürler ya da işaretler 46(2) maddesinin (f) bendinde atıfta bulunulan koşullar uyarınca üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları çerçevesinde 3. madde uyarınca bu Tüzük'e tabi olmayan kontroller veya işleyiciler tarafından sağlanan uygun güvencelerin var olduğunun gösterilmesi amacıyla oluşturulabilir. Söz konusu kontrolörler veya işleyiciler, veri sahiplerinin hakları ile ilgili olanlar da dahil olmak üzere uygun güvenceleri uygulamak üzere sözleşmeye bağlı veya diğer bağlayıcı belgeler vasıtasıyla bağlayıcı ve uygulanabilir taahhütlerde bulunur.

3. Belgelendirme gönüllülük esasına dayanır ve şeffaf bir süreç vasıtasıyla sağlanır.

4. Bu madde uyarınca sağlanan bir belgelendirme kontrolör ya da işleyicinin bu Tüzük'e uyma sorumluluğunu azaltmaz ve bu belgelendirme ile 55 veya 56. madde uyarınca yetkin olan denetim makamlarının görevleri ve yetkilerine hâlel gelmez.

5. Bu madde uyarınca sağlanan bir belgelendirme 43. maddede atıfta bulunulan belgelendirme organları veya yetkin denetim makamı tarafından 58(3) madde uyarınca söz konusu yetkin denetim makamı veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak sağlanır. Kriterlerin Kurul tarafından onaylandığı hallerde, ortak bir belgelendirme olan Avrupa Veri Koruma Mührü verilebilir.

6. İşleme faaliyetlerini belgelendirme mekanizmasına sunan kontrolör veya işleyici belgelendirme usulünün gerçekleştirilmesi için gereken tüm bilgiler ve işleme faaliyetlerine erişimi 43. maddede atıfta bulunulan belgelendirme organına veya, uygun olduğu hallerde, yetkin denetim makamına sağlar.

7. Belgelendirme bir kontrolör veya işleyiciye azami üç yıllık bir süre için sağlanır ve, ilgili gerekliliklerin yerine getirilmesine devam edilmesi koşuluyla, aynı koşullar altında, yenilenebilir. Belgelendirme gerekliliklerinin yerine getirilmediği veya artık yerine getirilmediği hallerde, belgelendirme, uygun olduğu hallerde, 43. maddede atıfta bulunulan belgelendirme organları veya yetkin denetim makamı tarafından geri çekilebilir.

8. Kurul tüm belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretlerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar.

4.20. Belgelendirme Organları (Madde 43)

1. Yetkin denetim makamının 57 ve 58. maddeler kapsamındaki görevleri ve yetkilerine halel gelmeksizin, veri koruma ile ilgili uygun bir uzmanlık seviyesine sahip olan belgelendirme organları, gerekmesi halinde 58(2) maddesinin (h) bendi uyarınca yetkilerinin kullanılmasını sağlamak üzere denetim makamını bilgilendirdikten sonra, belgelendirme sağlar ve belgelendirmeyi yeniler. Üye devletler bu belgelendirme organlarının aşağıdakilerin biri veya her ikisi tarafından akredite edilmesini sağlar:

(a) 55 veya 56. maddeler uyarınca yetkin olan denetim makamı;

(b) EN-ISO/IEC 17065/2012'ye uygun olarak (AT) 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü² uyarınca ve 55 ya da 56. madde uyarınca yetkin olan denetim makamı tarafından belirlenen ek gereklilikler uyarınca tayin edilen ulusal akreditasyon organı.

2. 1. paragrafta atıfta bulunulan belgelendirme organları, ancak aşağıdaki özellikleri taşımaları halinde, bu paragraf uyarınca akredite edilir:

(a) belgelendirme konusuna ilişkin bağımsızlıkları ve uzmanlıklarını yetkin denetim makamını tatmin edecek şekilde göstermiş olmaları;

(b) 42(5) maddesinde atıfta bulunulan ve 55 veya 56. madde uyarınca yetkin olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere riayet etmeyi taahhüt etmiş olmaları;

(c) veri koruma belgelendirmesi, mühürleri ve işaretlerinin verilmesi, düzenli aralıklarla gözden geçirilmesi ve geri çekilmesine ilişkin usuller oluşturmuş olmaları;

(d) belgelendirme veya belgelendirmenin bir kontrolör ya da işleyici tarafından uygulanmış olma veya uygulanma şekline ilişkin ihlallere yönelik şikayetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olmaları ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olmaları ve

(e) görev ve vazifelerinin bir çıkar çatışmasına neden olmadığını yetkin denetim makamını tatmin edecek şekilde göstermiş olmaları.

3. Belgelendirme organlarının bu maddenin 1 ve 2. bentlerinde atıfta bulunulan şekilde akreditasyonu 55 veya 56. madde uyarınca yetkin olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak gerçekleşir. Bu maddenin

1. paragrafının (b) bendi uyarınca akreditasyon yapılması halinde, bu gereklilikler (AT) 765/2008 sayılı Tüzük'te öngörülen gereklilikleri ve belgelendirme organlarının yöntemleri ve usullerinin açıklandığı teknik kuralları tamamlar.

4. 1. paragrafta atıfta bulunulan belgelendirme organları, kontrolör veya işleyicinin bu Tüzük'e uyum sorumluluğuna halel gelmeksizin, belgelendirmeye sonuçlanan uygun bir değerlendirmeden veya söz konusu belgelendirmenin geri çekilmesinden sorumludur. Akreditasyon azami beş yıllık bir süre için verilir ve, belgelendirme organının bu maddede ortaya konan gereklilikleri yerine getirmesi koşuluyla, aynı koşullar altında, yenilenebilir.

5. 1. paragrafta atıfta bulunulan belgelendirme organları talep edilen belgelendirmenin verilmesi veya geri çekilmesine ilişkin sebepleri yetkin denetim makamına sağlar.

6. Bu maddenin 3. paragrafında atıfta bulunulan gereklilikler ve 42(5) maddesinde atıfta bulunulan kriterler denetim makamı tarafından kolayca erişilebilecek bir formatta kamuya açıklanır. Denetim makamları da bu gereklilikleri ve kriterleri Kurula iletir. Kurul tüm belgelendirme mekanizmaları ve veri koruma mühürlerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar.

7. Bölüm VIII'e halel gelmeksizin, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya bir belgelendirme organı tarafından gerçekleştirilen eylemlerin bu Tüzük'ü ihlal ettiği hallerde, yetkin denetim makamı veya ulusal akreditasyon organı bu maddenin 1. paragrafı uyarınca bir belgelendirme organının akreditasyonunu kaldırır.

8. Komisyon 42(1) maddesinde atıfta bulunulan veri koruma belgelendirme mekanizmalarına yönelik olarak gerekliliklerin belirtilmesi amacıyla 92. madde uyarınca yetki devrine dayanan tasarrufları kabul etmeye yetkindir.

9. Komisyon belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretleri ve belgelendirme mekanizmaları, mühürleri ve işaretlerinin tanıtılması ve tanınmasıyla ilgili mekanizmalara ilişkin teknik standartların belirlendiği uygulama tasarrufları kabul edebilir. Bu uygulama tasarrufları 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

BÖLÜM 5. KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE VEYA ULUSLARARASI KURULUŞLARA AKTARILMASI

5.1. Aktarımlar İçin Genel Prensipler (Madde 44)

GDPR, kişisel verilerin AB içinde serbest dolaşımını sağlar. Ancak, kişisel verilerin AB üyesi ülke dışındaki bir ülkeye aktarılması, veri sahiplerinin haklarının korunması açısından risk oluşturabileceğinden, GDPR'da bu tür aktarımlara ilişkin özel hükümler düzenlenmiştir.

GDPR'ın 44. maddesine göre, kişisel verilerin AB üyesi ülke dışındaki bir ülkeye aktarılması, ancak aşağıdaki şartlardan birinin varlığı halinde hukuka uygun olabilir:

- **Aktarımın, AB Komisyonu tarafından yeterlilik kararı verilmiş bir ülkeye yapılması:** Avrupa Komisyonu, kişisel verilerin korunması açısından yeterli düzeyde koruma sağlayan ülkeleri belirlemek için bir değerlendirme süreci yürütür. Bu değerlendirme sonucunda, yeterlilik kararı verilen ülkelere aktarılan kişisel veriler, AB içinde aktarılmış gibi kabul edilir.
- **Aktarımın, standart sözleşme maddelerinin kullanılması:** Veri sorumlusu ve veri işleyen, Avrupa Komisyonu tarafından onaylanan standart sözleşme maddelerini kullanarak, kişisel verilerin aktarımını hukuka uygun hale getirebilir. Bu sözleşme maddeleri, kişisel verilerin korunmasına ilişkin temel güvenceleri içermektedir.
- **Aktarımın, belirli koşullara tabi olarak yapılması:** Kişisel verilerin aktarımı, aşağıdaki koşullara tabi olarak da hukuka uygun olabilir:
 - Aktarımın, veri sahibinin açık rızasına dayanması
 - Aktarımın, veri sorumlusunun veya veri işleyenin meşru menfaatleri için gerekli olması ve veri sahibinin temel hak ve özgürlüklerine zarar vermemesi
 - Aktarımın, bir hukuki yükümlülüğün yerine getirilmesi için gerekli olması
 - Aktarımın, bir kamu menfaatine hizmet etmesi için gerekli olması

GDPR'da, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması konusunda veri sorumlularına ve veri işleyenlere bazı yükümlülükler de getirilmiştir. Bu yükümlülükler, kişisel verilerin korunmasını sağlamak amacıyla veri sorumluları ve veri işleyenlerin belirli önlemleri almasını gerektirmektedir.

GDPR'da kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin hükümler, veri sahiplerinin haklarının korunması açısından önemlidir. Bu hükümler, veri sorumluları ve veri işleyenlerin, kişisel verilerin aktarılması sırasında veri sahiplerinin haklarını korumak için gerekli önlemleri almasını zorunlu kılmaktadır.

Rıza: Kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabilmesi için, kişisel veri sahibinin açık rızasını alması gerekir. Açık rıza, serbestçe ve aydınlatılmış bir şekilde verilen, belirli, açık ve meşru bir amaçla sınırlı bir onaydır.

Yeterlilik Kararı: Avrupa Komisyonu, kişisel verilerin korunması açısından yeterli veri koruma düzeyine sahip olan üçüncü ülkeleri belirlemiştir. Bu ülkeler, GDPR'a uygun bir veri koruma mevzuatı ve uygulamalarını haiz olan ülkelerdir.

Özel Veri Aktarımı Sözleşmeleri: Standart sözleşme maddeleri (SCC'ler), veri sorumluları ve veri işleyenler tarafından, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasında kullanılabilecek sözleşme maddeleridir. SCC'ler, AB Komisyonu tarafından hazırlanmış ve onaylanmıştır.

Özel Hükümler: AB hukuku kapsamında yer alan özel hükümler, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasında kullanılabilecek özel şartlardır. Bu hükümler, örneğin bir AB-üçüncü ülke arasındaki veri paylaşımı anlaşmasında yer alabilir.

GDPR'ın Üçüncü Ülkelere Veri Aktarımı Üzerindeki Etkileri

GDPR'ın üçüncü ülkelere veri aktarımı üzerindeki etkileri şu şekilde özetlenebilir:

- Açık rıza şartının genişletilmesi: GDPR, kişisel verilerin üçüncü ülkelere aktarılabilmesi için açık rıza şartını genişletmiştir. Buna göre, artık kişisel verilerin üçüncü ülkelere aktarılabilmesi için, kişisel veri sahibinin açık rızasının açık, belirli, bilgilendirilmiş ve özgür iradeyle verilmiş olması gerekir.
- Yeterlilik kararlarının önemi: GDPR, yeterlilik kararlarının önemini artırmıştır. Buna göre, kişisel verilerin üçüncü ülkelere aktarılabilmesi için, ilgili üçüncü ülkenin yeterli bir veri koruma düzeyine sahip olduğunun Avrupa Komisyonu tarafından kabul edilmesi gerekir.
- Özel veri aktarımı sözleşmelerinin yaygınlaşması: GDPR, özel veri aktarımı sözleşmelerinin yaygınlaşmasını teşvik etmiştir. SCC'ler, kişisel verilerin üçüncü ülkelere aktarılmasında kullanılabilecek en yaygın sözleşme maddeleridir.

Üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarıldıktan sonra işlenmekte olan veya işlenmeye yönelik kişisel verilerin aktarılması, ancak bu Politika'nın diğer hükümlerine tabi olarak, bu bölümde belirtilen koşullara kontrolör ve işlemci tarafından uyulması halinde üçüncü ülkeden veya uluslararası bir kuruluştan başka bir üçüncü ülkeye veya başka bir uluslararası kuruluşa kişisel verilerin aktarılması, ileriye dönük aktarımlar da dahil olmak üzere gerçekleşir.

Bu Politika ile güvence altına alınan gerçek kişilerin koruma düzeyinin zedelenmemesi için bu bölümdeki tüm hükümler uygulanır.

Bilge Bank A.Ş.'nin uluslararası niteliği göz önünde bulundurularak ve hizmetlerinin kalitesini optimize etmek için kişisel verileri, kişisel verilerin korunması mevzuatının Avrupa Birliği'nde uygulanandan farklı olduğu üçüncü ülkelere veya uluslararası kuruluşlara aktarabilir.

Böyle bir durumda, ilgili ülke Avrupa Komisyonu tarafından yeterli düzeyde kişisel veri koruması sağladığı resmi olarak tanınmadıkça Bilge Bank A.Ş., aktarılan kişisel verilerin uygun standart sözleşme hükümleri veya belirtilen diğer garantilerle korunmasını sağlayacaktır.

Ayrıca bu transferler, değiştirildiği şekliyle 5 Nisan 1993 tarihli finans sektörü Kanunu'nun 41. Maddesine uygun olarak yapılacaktır. Bu tür veri transferleri, kişisel verilerin korunmasını ve güvenliğini sağlamaya yönelik şart ve garantilere uygun olarak gerçekleştirilecektir.

GDPR'a göre, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması ancak aşağıdaki şartlardan birinin varlığı halinde mümkündür:

- **Aktarımın yeterlilik kararı kapsamında olması:** Avrupa Komisyonu, bazı üçüncü ülkeleri yeterlilik kararı ile AEA ile eşdeğer bir veri koruma düzeyi sağladığına karar verebilir. Bu durumda, kişisel verilerin bu ülkelere aktarılması için herhangi bir ek şarta gerek yoktur.
- **Aktarımın standart sözleşme maddelerinin kullanılması:** Avrupa Komisyonu, kişisel verilerin üçüncü ülkelere aktarılmasının güvence altına alınması için standart sözleşme maddeleri (SCC) hazırlamıştır. Veri sorumluları, SCC'leri kullanarak kişisel verilerini üçüncü ülkelere aktarabilirler.

SCC'ler, veri sorumlusu ile veri işleyen arasında imzalanan sözleşmelere eklenir. SCC'ler, veri sorumlusunun ve veri işleyenin kişisel verilerini üçüncü ülkelere aktarırken uymaları gereken güvenceleri belirler.

- **Aktarımın bir veri koruma sertifikasyon mekanizması kapsamında olması:** Veri sorumluları, kişisel verilerini üçüncü ülkelere aktarmak için bir veri koruma sertifikasyon mekanizmasına başvurabilirler. Bu mekanizmalar, veri sorumlularının kişisel verilerini üçüncü ülkelere aktarırken uymaları gereken güvenceleri belirler.
- **Aktarımın özel veri koruma önlemlerine tabi olması:** Veri sorumluları, kişisel verilerini üçüncü ülkelere aktarırken özel veri koruma önlemleri uygulayabilirler. Bu önlemler, kişisel verilerin korunmasını sağlamaya yönelik teknik ve/veya idari tedbirlerdir.

Özel veri koruma önlemlerine örnek olarak, veri şifreleme, veri anonimleştirme, veri saklama süresi sınırlandırması gösterilebilir.

GDPR'a göre, veri sorumluları, kişisel verilerini üçüncü ülkelere aktarmadan önce, aktarımın hukuka uygunluğunu değerlendirmelidir. Bu değerlendirmede, yukarıda belirtilen şartlar göz önünde bulundurulmalıdır.

5.2. Yeterlilik Kararına Dayalı Aktarımlar (Madde 45)

1. Kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılması, Komisyonun üçüncü ülkenin, o üçüncü ülke içindeki bir bölgenin veya bir veya daha fazla belirli sektörün veya söz konusu uluslararası kuruluşun yeterli düzeyde koruma sağladığına karar verdiği durumlarda gerçekleşebilir. Böyle bir aktarım, herhangi bir özel izin gerektirmez.
2. Koruma seviyesinin yeterliliğini değerlendirirken, Komisyon özellikle aşağıdaki unsurları dikkate alacaktır:
 - a. Hukukun üstünlüğü, insan haklarına ve temel özgürlüklere saygı, kamu güvenliği, savunma, milli güvenlik ve ceza hukuku ve kamu otoritelerinin kişisel verilere erişimi ile ilgili olmak üzere hem genel hem de sektörel ilgili mevzuat ve bu mevzuatın uygulanması, veri koruma kuralları, meslek kuralları ve güvenlik kişisel verilerin o ülkede veya uluslararası kuruluşta uyulması gereken başka bir üçüncü ülkeye veya uluslararası kuruluşa daha sonra aktarılmasına ilişkin kurallar da dahil olmak üzere önlemler, içtihatlar, kişisel verileri aktarılmakta olan veri sahipleri için etkin ve uygulanabilir veri sahibi haklarının yanı sıra etkin idari ve adli tazminat;
 - b. Üye Devletlerin denetim otoriteleri ile üçüncü ülkede veya uluslararası bir kuruluşun tabi olduğu bir veya daha fazla bağımsız denetim otoritesinin, yeterli uygulama yetkileri de dahil olmak üzere veri koruma kurallarına uyumu sağlama ve uygulama, veri konularına haklarını kullanmada yardımcı olma ve danışmanlık yapma ve işbirliği yapma sorumluluğu ile varlığı ve etkin işleyişi
 - c. İlgili üçüncü ülke veya uluslararası kuruluşun, özellikle kişisel verilerin korunmasına ilişkin olarak, çok taraflı veya bölgesel sistemlere katılımının yanı sıra yasal olarak bağlayıcı sözleşmeler veya araçlardan kaynaklanan uluslararası taahhütler veya diğer yükümlülükler.
3. Komisyon, koruma düzeyinin yeterliliğini değerlendirdikten sonra, üçüncü bir ülkenin, bir bölgenin veya üçüncü bir ülke içindeki bir veya daha fazla belirli sektörün veya uluslararası bir kuruluşun, bu bölümün 2. maddesi anlamında yeterli düzeyde

koruma sağladığına kanunun uygulanması yoluyla karar verebilir. Uygulama yasası, en az dört yılda bir, üçüncü ülke veya uluslararası kuruluşdaki tüm ilgili gelişmeleri dikkate alacak periyodik bir gözden geçirme mekanizması sağlayacaktır. Uygulama yasası, bölgesel ve sektörel uygulamasını belirleyecek ve uygulanabilir olduğunda, bu bölümün 2. maddesinin (b) bendinde belirtilen denetim otoritesini veya makamlarını belirleyecektir. Uygulama kanunu, 93. maddede belirtilen inceleme usulüne uygun olarak kabul edilir.

4. Komisyon, bu bölümün 3. maddesi uyarınca alınan kararların işleyişini etkileyebilecek üçüncü ülke ve uluslararası kuruluşlardaki gelişmeleri ve 95/46/EC sayılı Direktifin 25(6) maddesine dayanarak alınan kararları sürekli olarak izleyecektir.
5. Komisyon, mevcut bilgilerin ortaya koyduğu durumlarda, özellikle bu bölümün 3. maddesinde atıfta bulunulan incelemeyi takiben, üçüncü bir ülke, bir bölge veya üçüncü bir ülke veya uluslararası bir kuruluş içindeki belirli bir veya daha fazla sektörün, bu bölümün 2. maddesi anlamında artık yeterli düzeyde koruma sağlamadığını, bu bölümün 3. maddesinde belirtilen kararı, gerektiğinde, geriye dönük etkin etkisi olmayan fiillerin uygulanması yoluyla yürürlükten kaldırabilir, değiştirebilir veya askıya alabilir. Bu eylemleri uygulayanlar, Madde 93 (2)'de belirtilen inceleme usulüne uygun olarak kabul edilir. Komisyon, usulüne uygun olarak gerekçelendirilmiş zorunlu aciliyet gerekçeleriyle, Madde 93 (3)'te belirtilen usule uygun olarak derhal uygulanabilir uygulama eylemlerini kabul eder.
6. Komisyon, 5. madde uyarınca alınan karara yol açan durumu düzeltmek amacıyla üçüncü ülke veya uluslararası kuruluşla istişarelerde bulunacaktır.
7. Bu bölümün 5. maddesi uyarınca alınan bir karar, kişisel verilerin üçüncü ülkeye, o üçüncü ülke içindeki belirli bir bölgeye veya bir veya daha fazla sektöre veya 46 ila 49. Maddeler uyarınca söz konusu uluslararası kuruluşla aktarılmasına hâlel getirmez.
8. Komisyon, Avrupa Birliği'nin Resmi Gazetesinde ve internet sitesinde, üçüncü bir ülke içindeki üçüncü ülkelerin, bölgelerin ve belirli sektörlerin ve yeterli düzeyde korumanın sağlandığına veya sağlanmadığına karar verdiği uluslararası kuruluşların bir listesini yayınlayacaktır.
9. Komisyon tarafından 95/46/ EC Sayılı Direktifin 25 (6) maddesine dayanarak alınan kararlar, bu bölümün 3. veya 5. maddesi uyarınca kabul edilen bir Komisyon Kararı ile değiştirilene, değiştirilene veya yürürlükten kaldırılana kadar yürürlükte kalacaktır.

5.3. Uygun Güvencelere Tabi Aktarımlar (Madde 46)

1. Madde 45 (3) uyarınca bir kararın bulunmaması halinde, bir denetleyici veya işlemci, kişisel verileri ancak denetleyici veya işlemci uygun güvenceler sağlamışsa ve uygulanabilir veri sahibi hakları ve veri sahipleri için etkili yasal yolların mevcut olması koşuluyla üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarabilir.
2. Yukarıda atıfta bulunulan uygun güvenceler, bir denetim otoritesinden herhangi bir özel izin gerektirmeksizin aşağıdakiler tarafından sağlanabilir:
 - a. kamu otoriteleri veya organları arasında yasal olarak bağlayıcı ve uygulanabilir bir araç
 - b. madde 47 uyarınca bağlayıcı kurumsal kurallar
 - c. madde 93(2)'de belirtilen inceleme usulüne uygun olarak Komisyon tarafından kabul edilen standart veri koruma maddeleri
 - d. bir denetim otoritesi tarafından kabul edilen ve 93üncü Maddenin(2) bendinde belirtilen inceleme usulü uyarınca Komisyon tarafından onaylanan standart veri koruma maddeleri
 - e. 40. Madde uyarınca onaylanmış bir davranış kuralları, veri sahiplerinin hakları da dahil olmak üzere uygun önlemleri uygulamak için üçüncü ülkedeki denetleyicinin veya işlemcinin bağlayıcı ve uygulanabilir taahhütleriyle birlikte
 - f. madde 42 uyarınca onaylanmış bir belgelendirme mekanizması ve üçüncü ülkedeki denetleyici veya işlemcinin veri sahiplerinin hakları da dahil olmak üzere uygun güvenceleri uygulama konusundaki bağlayıcı ve uygulanabilir taahhütleri.
3. Yetkili denetim otoritesinin iznine tabi olarak, yukarıda belirtilen uygun güvenceler, özellikle aşağıdakiler tarafından da sağlanabilir:
 - a. üçüncü ülke veya uluslararası kuruluştaki kişisel verilerin denetleyicisi veya işleyicisi ile denetleyicisi, işleyicisi veya alıcısı arasındaki sözleşme hükümleri
 - b. kamu otoriteleri veya organları arasında uygulanabilir ve etkin veri sahibi haklarını içeren idari düzenlemelere eklenecek hükümler.

4. Denetim otoritesi, bu bölümün 3. maddesinde belirtilen hallerde 63. maddede belirtilen tutarlılık mekanizmasını uygulayacaktır.
5. 95/46/ EC sayılı Direktifin 26. Maddesinin (2) bendine dayanan bir Üye Devlet veya denetim otoritesinin yetkileri, gerektiğinde bu denetim otoritesi tarafından değiştirilene veya yürürlükten kaldırılana kadar geçerli kalır. Komisyon tarafından 95/46/EC sayılı Direktifin 26. Maddesinin (4) bendine dayanarak alınan kararlar, bu bölümün 2. maddesi uyarınca kabul edilen bir Komisyon Kararı ile gerekirse değiştirilene veya yürürlükten kaldırılana kadar yürürlükte kalacaktır.

5.4. Bağlayıcı Kurumsal Kurallar (Madde 47)

1. Yetkili denetim otoritesi, bağlayıcı kurumsal kuralları, madde 63'te belirtilen tutarlılık mekanizmasına uygun olarak, aşağıdaki şartlarla onaylayacaktır:
 - a. Yasal olarak bağlayıcıdır ve çalışanları da dahil olmak üzere ortak bir ekonomik faaliyette bulunan teşebbüsler grubu veya şirketler grubuyla ilgili her üye için geçerlidir ve bunlar tarafından uygulanır.
 - b. Kişisel verilerinin işlenmesiyle ilgili olarak veri sahiplerine açıkça uygulanabilir haklar vermek.
 - c. 2. maddede belirtilen şartlar yerine getirilmelidir.
2. 1. maddede atıfta bulunulan bağlayıcı şirket kuralları en az:
 - a. ortak bir ekonomik faaliyette bulunan şirketler grubunun veya şirket grubu üyelerinin her birinin yapısı ve iletişim bilgileri;
 - b. kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri konularının türü ve söz konusu üçüncü ülke veya ülkelerin tanımlanması dahil olmak üzere veri aktarımları veya aktarımlar kümesi;
 - c. hem dahili hem de harici olarak yasal olarak bağlayıcı yapıları;
 - d. bağlayıcı kurumsal kurallara bağlı olmayan kuruluşlara genel veri koruma ilkelerinin uygulanması, özellikle amaç sınırlaması, verilerin en aza indirilmesi, sınırlı saklama süreleri, veri kalitesi, tasarım gereği ve varsayılan olarak veri koruması, işlenmesi için yasal dayanak, özel kişisel veri kategorilerinin işlenmesi, veri güvenliğini sağlamaya yönelik önlemler ve veri güvenliğine yönelik ileriye dönük aktarımlara ilişkin gereklilikler;

- e. 22. madde uyarınca profil oluřturma, yetkili denetim otoritesine ve Üye Devletlerin yetkili mahkemelerine řikâyetle bulunma hakkı da dahil olmak üzere, yalnızca otomatik işlemeye dayalı kararlara tabi olmama hakkı dahil olmak üzere, veri sahiplerinin işleme konusundaki hakları ve bu hakları kullanma araçları 79. maddeye uygun olarak ve bağlayıcı kurumsal kuralların ihlali için tazminat ve uygun olduğunda tazminat almak;
- f. Bankada kurulmamış ilgili herhangi bir üye tarafından bağlayıcı kurumsal kuralların ihlal edilmesinden sorumlu bir Üye Devletin topraklarında kurulan denetleyici veya işleyici tarafından kabul edilmesi; denetleyici veya işleyici, ancak bu üyenin bağlayıcı kurumsal kuralların ihlal edilmesinden sorumlu olduğunu kanıtlaması halinde, bu sorumluluktan tamamen veya kısmen muaf tutulacaktır. Hasara yol açan olaydan sorumlu değildir;
- g. bu fıkranın (d), (e) ve (f) bentlerinde belirtilen hükümler başta olmak üzere bağlayıcı kurumsal kurallara ilişkin bilgilerin, 13. ve 14. Maddelere ek olarak veri sahiplerine nasıl sağlandığı;
- h. 37. maddeye göre belirlenen herhangi bir veri koruma görevlisinin veya işletmeler grubu veya ortak bir ekonomik faaliyette bulunan işletmeler grubu içindeki bağlayıcı kurumsal kurallara uygunluğun izlenmesinden sorumlu başka herhangi bir kişi veya kuruluşun görevleri ile eğitim ve řikayetlerin ele alınmasının izlenmesi;
- i. řikayet prosedürleri;
- j. bağlayıcı kurumsal kurallara uygunluğun doğrulanmasını sağlamak için ortak bir ekonomik faaliyette bulunan işletmeler grubu veya işletmeler grubu içindeki mekanizmalar. Bu tür mekanizmalar, veri koruma denetimlerini ve veri sahibinin haklarını korumak için düzeltici faaliyetlerin sağlanmasına yönelik yöntemleri içerecektir. Bu doğrulamanın sonuçları, (h) bendinde belirtilen kişi veya kuruluřa ve bir grup işletmenin veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun kontrol eden işletmesinin kuruluna iletilmeli ve talep üzerine yetkili denetim otoritesine sunulmalıdır;
- k. kurallardaki deęişikliklerin raporlanması ve kaydedilmesi ve bu deęişikliklerin denetim otoritesine bildirilmesi için mekanizmalar;

1. özellikle (j) bendinde belirtilen önlemlerin doğrulanmasının sonuçlarını denetim otoritesine sunarak, işletmeler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun herhangi bir üyesinin uygunluğunu sağlamak için denetim otoritesi ile işbirliği mekanizması;
 - m. üçüncü bir ülkede, bağlayıcı kurumsal kuralların sağladığı garantiler üzerinde önemli bir olumsuz etkisi olması muhtemel olan işletmeler grubunun veya ortak ekonomik faaliyette bulunan işletmeler grubunun bir üyesinin tabi olduğu herhangi bir yasal gerekliliği yetkili denetim otoritesine raporlama mekanizmaları;
 - n. kişisel verilere sürekli veya düzenli erişimi olan personele uygun veri koruma eğitimi.
3. Komisyon, bu Madde kapsamında bağlayıcı kurumsal kurallar için denetçiler, işlemciler ve denetim otoriteleri arasında bilgi alışverişinin biçimini ve prosedürlerini belirleyebilir. Bu eylemleri uygulayanlar, Madde 93(2)'de belirtilen inceleme usulüne uygun olarak kabul edilir.

5.5. Sendika Yasalarında İzin Verilmeyen Aktarımlar veya Açıklamalar (Madde 48)

Bir mahkemenin veya mahkemenin herhangi bir kararı ve bir denetleyici veya işlemcinin kişisel verileri aktarmasını veya ifşa etmesini gerektiren üçüncü bir ülkenin idari makamının herhangi bir kararı, ancak talep eden üçüncü ülke, Banka veya Üye Devlet arasında yürürlükte olan karşılıklı hukuki yardım anlaşması gibi uluslararası bir anlaşmaya dayanıyorsa, bu fasıl uyarınca aktarım için diğer gerekçelere hâlel getirmeksizin herhangi bir şekilde tanınabilir veya uygulanabilir.

5.6. Belirli Durumlar İçin İstisnalar (Madde 49)

1. Madde 45 (3) uyarınca bir yeterlilik kararının veya bağlayıcı şirket kuralları da dahil olmak üzere Madde 46 uyarınca uygun güvencelerin bulunmaması durumunda, kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılması veya bir dizi aktarımı yalnızca aşağıdaki koşullardan birinde gerçekleşir:
 - a. veri sahibi, bir yeterlilik kararının ve uygun güvencelerin bulunmaması nedeniyle veri sahibi için bu tür transferlerin olası riskleri hakkında bilgilendirildikten sonra, önerilen aktarıma açıkça rıza göstermiştir;

- b. aktarım, veri sahibi ile denetleyici arasındaki bir sözleşmenin yerine getirilmesi veya veri sahibinin talebi üzerine alınan sözleşme öncesi önlemlerin uygulanması için gereklidir;
- c. aktarım, kontrolör ile başka bir gerçek veya tüzel kişi arasında veri konusu yararına yapılan bir sözleşmenin imzalanması veya ifası için gereklidir;
- d. aktarım, kamu yararının önemli nedenleri için gereklidir;
- e. aktarım, yasal taleplerin oluşturulması, uygulanması veya savunulması için gereklidir;
- f. aktarım, veri sahibinin fiziksel veya yasal olarak rıza gösteremediği durumlarda, veri sahibinin veya diğer kişilerin hayati çıkarlarını korumak için gereklidir;
- g. aktarım, Banka veya Üye Devlet yasalarına göre kamuya bilgi vermeyi amaçlayan ve ya genel olarak halk tarafından ya da meşru bir menfaat gösterebilecek herhangi bir kişi tarafından istişareye açık olan bir sicilden yapılır, ancak yalnızca Banka veya Üye tarafından belirlenen koşulların gerektirdiği ölçüde İstişare için devlet hukuku belirli bir durumda yerine getirilir.

Bağlayıcı şirket kurallarına ilişkin hükümler de dahil olmak üzere 45. veya 46. Maddedeki bir hükmün esas alınmadığı ve bu fıkranın birinci maddesinde belirtilen belirli bir duruma ilişkin derogasyonların hiçbirinin geçerli olmadığı durumlarda, üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarım ancak aşağıdaki durumlarda gerçekleşebilir: aktarım tekrarlı değildir, yalnızca sınırlı sayıda veri sahibini ilgilendirir, denetleyici tarafından takip edilen ve veri sahibinin çıkarları veya hak ve özgürlükleri tarafından geçersiz kılınmayan meşru çıkarları zorlamak amacıyla gereklidir, denetleyici, veri aktarımını çevreleyen tüm koşulları değerlendirmiş ve bu değerlendirmeye dayanarak kişisel verilerin korunmasına ilişkin uygun güvenceler sağlamıştır. Kontrolör, devir hakkında denetim otoritesini bilgilendirecektir. Kontrolör, 13. ve 14. Maddelerde atıfta bulunulan bilgileri sağlamanın yanı sıra, veri sahibini transfer hakkında ve takip edilen zorlayıcı meşru menfaatler hakkında bilgilendirecektir.

BİLGE BANK A.Ş.

- 2. Birinci maddenin (g) bendi uyarınca yapılan bir aktarım, kişisel verilerin tamamını veya sicilde yer alan kişisel verilerin tüm kategorilerini kapsamaz. Kayıt defterinin meşru menfaati olan kişiler tarafından istişareye yönelik olması durumunda, aktarım yalnızca bu kişilerin talebi üzerine veya alıcı olacaklarsa yapılır.
- 3. Birinci maddenin (a), (b) ve (c) bentleri ile ikinci madde, kamu otoritelerinin kamu yetkilerini kullanmaları sırasında yürüttükleri faaliyetler için geçerli olmayacaktır.
- 4. Birinci maddenin (d) bendinde belirtilen kamu yararı, Banka hukukunda veya denetçinin tabi olduğu Üye Devlet hukukunda muhasebeleştirilir.
- 5. Bir yeterlilik kararının bulunmaması halinde, Banka veya Üye Devlet yasaları, kamu yararı açısından önemli nedenlerle, belirli kategorilerdeki kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasına açıkça sınırlar koyabilir. Üye Devletler bu hükümleri Komisyona bildireceklerdir.
- 6. Denetleyici veya işleyici, değerlendirmeyi ve belirtilen uygun güvenceleri, 30. Maddede birinci maddenin ikinci alt maddesinde belirtilen kayıtlarda belgeleyecektir.

5.7. Kişisel Verilerin Korunması İçin Uluslararası İşbirliği (Madde 50)

1. Üçüncü ülkeler ve uluslararası kuruluşlarla ilgili olarak, komisyon ve denetim otoriteleri aşağıdaki konularda uygun adımları atacaktır:
 - a. Kişisel verilerin korunmasına yönelik mevzuatın etkin bir şekilde uygulanmasını kolaylaştırmak için uluslararası işbirliği mekanizmaları geliştirmek;
 - b. Kişisel verilerin ve diğer temel hak ve özgürlüklerin korunmasına yönelik uygun güvencelere tabi olarak, bildirim, şikâyet yönlendirme, soruşturma yardımı ve bilgi alışverişi dahil olmak üzere kişisel verilerin korunmasına ilişkin mevzuatın uygulanmasında uluslararası karşılıklı yardım sağlamak;
 - c. İlgili paydaşları, kişisel verilerin korunmasına ilişkin mevzuatın uygulanmasında uluslararası işbirliğini ilerletmeyi amaçlayan tartışma ve faaliyetlere dahil etmek;
 - d. Üçüncü ülkelerle yargı ihtilafları da dahil olmak üzere kişisel verilerin korunması mevzuatı ve uygulamalarının değişimini ve belgelenmesini teşvik etmek.

5.8. Veri Aktarımı

5.8.1. Konsolide Denetim Çerçevesinde

Bilge Bank A.Ş., konsolide denetim yükümlülüklerine uyum kapsamında, kara para aklamanın önlenmesi ve bunlarla mücadele ile grup içindeki terörizmin finansmanı ile ilgili temel kredi risk ve risklerinin azaltılması ihtiyacını karşılamak amacıyla veri alışverişinde bulunmaktadır. Bu nedenle, Banka, kredi riskini yönetimi bağlamında, risklerin önceden değerlendirilmesi, müşterinin önemli miktarda ve / veya süre için kredi talep etmesi durumunda değerlendirilmesi veya kredi riskinin izlenmesi ile ilgili verileri iletebilir (özellikle marjın yetersiz olması, fazla çekilmiş bir hesap veya bir limitin aşılması durumunda).

5.8.2. Üçüncü Taraflara

Sizinle yapılan sözleşmenin yönetimi çerçevesinde ve sunulan hizmetlerin ve finansal araçların türüne bağlı olarak, Bilge Bank A.Ş.'nin yurtiçi ve yurtdışında da veri paylaşması gerekebilir:

- Bankanın ticaret yapabileceği devredilebilir menkul kıymetler, para birimleri, opsiyonlar, vadeli işlemler ve diğer vadeli sözleşmelerde herhangi bir piyasa veya borsa ticareti ile bunlarla ilişkili herhangi bir takas odası ve menkul kıymetlerin teslimi için araçlar
- Yurtiçi veya yurtdışında finansal araçların herhangi bir saklayıcısı, alt saklayıcısı, komisyoncusu, ihraççısı veya destekçisi
- Kredi kartı verenler ve güvenli ödeme sistemleri
- Ödeme mesajlarının işlenmesinde yer alan herhangi bir üçüncü taraf (talimat veren taraf, yararlanıcı, hesap sahibi, muhabir bankalar, aracı bankalar)
- Özel sermaye fonları da dahil olmak üzere yönetim şirketleri, yöneticiler veya yöneticiler, yerel veya yabancı toplu yatırım planları
- Yurtiçi veya yurtdışında, alt saklama sözleşmelerine dahil olan veya dahil olması muhtemel herhangi bir finans kurumunun yanı sıra kredi referansları sağlayan finansal derecelendirme kuruluşları
- Yurtiçi veya yurtdışında, bu tür verileri herhangi bir yasa veya yönetmelik (sigortacılar, denetçiler, avukatlar, muhasebeciler) uyarınca talep etmeye yetkili herhangi bir kişi veya kuruluş

5.8.3. Hizmet Sağlayıcılara

Yürürlükteki yasa ve yönetmeliklerin izin verdiği ölçüde, Bilge Bank A.Ş. yurtiçi veya yurtdışındaki hizmet sağlayıcıları aşağıdakiler gibi belirli faaliyetleri dış kaynak olarak kullanmak için kullanabilir.

Muhasebe, bilgisayar donanımının sağlanması, bilgi sistemleri ve altyapısının yönetimi, arka ofis yönetimi, altın ve değerli metallerin yatırılması, veri arşivleme, posta gönderme, nakliye hizmetleri vb. acenteler olarak ve Banka ile imzalanan anlaşma uyarınca, hizmet sağlayıcıların tümü gizlilik ve veri koruma görevine bağlıdır. Kişisel verilerin yurtdışına aktarılmasının gerekli olduğu durumlarda Bilge Bank A.Ş., ilgili ülkenin yeterli düzeyde korumayı garanti etmesini veya veri koruma otoritesi tarafından tanınan standart sözleşme maddelerini sonuçlandırmasını sağlar.

5.8.4. Yetkililere, Düzenleyicilere veya Kamu Kurumlarına

Çok özel durumlarda Bilge Bank A.Ş., özellikle kara para aklama ve terörizmin finansmanı ile mücadeleyle ilişkin düzenlemeler, uluslararası yaptırımlar ve ambargolara ilişkin kurallar, pay sahiplerinin haklarının kullanılmasına ilişkin kurallar veya yürürlükteki diğer hususlar ile ilgili olarak verileri düzenleyiciye veya Bankanın tabi olduğu herhangi bir denetim otoritesine iletir.

Özellikle, meşru menfaatlerimizi korumak için gerekirse ihtiyati tedbir veya talep üzerine yurtiçi veya yurtdışında ilgili verileri ifşa etmemiz gerekebilir.

Müşterinin Bankaya karşı açtığı sahipsiz varlıkların, taleplerin veya yasal işlemlerin yönetimi, olaylarından biri meydana gelirse Bankanın taleplerini garanti altına almalı ve

müşteri veya üçüncü şahıslar tarafından devredilen menkul kıymetleri elden çıkarmalı, Bankanın Müşteriye karşı taleplerinin geri kazanılmasını sağlamalıdır.

5.8.5. Kişisel Verilerin Yurt Dışına Aktarılması

Banka, aşağıdakiler dahil olmak üzere kişisel verileri yurt dışında ifşa edebilir, iletebilir, aktarabilir ve / veya saklayabilir:

- Devredilen bir kamu menfaatini korumak için transferin gerekli olduğu durumlarda;
- Transferin, Bankanın mevcut veya gelecekteki bir iddiayı oluşturmamasını, kullanmasını veya savunmasını sağlamak veya Bankanın yurt içi veya yurt dışında bir kamu otoritesi tarafından soruşturmayla karşı karşıya kalmasını sağlamak için gerekli olduğu durumlarda;
- İş ilişkisine doğrudan veya dolaylı olarak ilişkin sözleşmelerin sonuçlandırılması veya ifasıyla bağlantılı olarak (yani bir Müşteriyle, İlgili bir Kişiyle veya üçüncü bir tarafla yapılan, ancak bir Müşterinin ve / veya İlgili bir Kişinin çıkarına olan bir sözleşme); veya
- Yürürlükteki yasaların usulüne uygun olarak öngördüğü istisnai durumlarda (ör. Belirli borsa işlemlerinin açıklanması).



BİLGE BANK A.Ş.

BÖLÜM 6. BAĞIMSIZ DENETİM OTORİTELERİ

6.1. Denetim Otoritesi (Madde 51)

Her Üye Devlet, gerçek kişilerin temel hak ve özgürlüklerini korumak ve kişisel verilerin AB içerisinde serbest akışını kolaylaştırmak amacıyla, bu Tüzüğün uygulanmasını izlemekle sorumlu bir veya daha fazla bağımsız kamu makamını sağlar. Bu makamlar topluca "denetim makamları" olarak anılır.

Her denetim makamı, bu Tüzüğün Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunur. Bu amaçla, denetim makamları Bölüm VII'ye göre birbirleriyle ve Komisyon ile işbirliği yapar.

Bir Üye Devlet, birden fazla denetim makamının bulunması durumunda, bu makamları Kurulda temsil edecek denetim makamını atar ve diğer makamların tutarlılığına ilişkin kurallara uymasını sağlamak için 63. maddeye uygun bir mekanizma oluşturur.

6.2. Bağımsızlık (Madde 52)

6.2.1 Makamının Bağımsızlığı

Her Denetim Makamı, bu Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken tam bağımsız hareket eder.

Her Denetim Makamının üyesi veya üyeleri, bu Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken, doğrudan veya dolaylı dış etkilere uzak durur ve kimseden talimat istemez veya alamaz.

Her Denetim Makamının üyesi veya üyeleri, görevleriyle bağdaşmayan herhangi bir eylemden kaçınır ve görev süreleri boyunca, kazanç getirir veya getirmese bile uyumsuz herhangi bir işle meşgul olmaz.

Her Üye Devlet, her Denetim Makamına, görevlerinin etkili bir şekilde yerine getirilmesi ve yetkilerinin kullanılması için gerekli insan, teknik ve mali kaynaklar, tesisler ve altyapıyı sağlar. Bu, Yönetim Kurulu ile işbirliği ve katılım içinde, karşılıklı yardım bağlamında gerçekleştirilecek olanlar da dahil olmak üzere geçerlidir.

Her Üye Devlet, her Denetim Makamının, ilgili Denetim Makamı üyesi veya üyelerinin münhasır talimatına tabi olacak kendi personelini seçmesini ve bu personele sahip olmasını sağlar.

Her Üye Devlet, her Denetim Makamının bağımsızlığını etkilemeyen mali kontrol altında olmasını sağlar ve genel devlet veya ulusal bütçenin bir parçası olabilecek ayrı, yıllık kamu bütçelerine sahip olmasını temin eder.

6.3. Denetleyici Makam Üyeleri İçin Genel Koşullar (Madde 53)

Üye Devletler, Bilge Bank A.Ş. Denetim Makamının her bir üyesinin şeffaf bir prosedür aracılığıyla aşağıdakiler tarafından atanmasını sağlayacaklardır:

Parlamentoları;

Hükümetleri;

Devlet Başkanları; veya

Üye Devlet hukuku kapsamında atama yapmakla görevlendirilen bağımsız bir organ.

Her üye, özellikle kişisel verilerin korunması alanında, görevlerini yerine getirmek ve yetkilerini kullanmak için gerekli nitelik, deneyim ve becerilere sahip olacaktır.

Bir üyenin görevleri, ilgili Üye Devletin kanunlarına uygun olarak görev süresinin sona ermesi, istifa veya zorunlu emeklilik durumunda sona erecektir.

Bir üye ancak ciddi suiistimal halinde veya görevin ifası için gerekli şartları artık yerine getirmiyorsa üyelikten çıkarılır.

Her Üye Devlet, Bilge Bank A.Ş. Denetim Makamının bağımsızlığını etkilemeyen mali kontrol altında olmasını sağlar ve genel devlet veya ulusal bütçenin bir parçası olabilecek ayrı, yıllık kamu bütçelerine sahip olmasını temin eder.

6.4. Denetim Otoritesinin Oluşumuna İlişkin Kurallar (Madde 54)

Her Üye Devlet, aşağıdakilerin tamamını kanunla sağlayacaktır:

a. Her denetim makamının kurulması;

b. Her bir denetim makamının üyesi olarak atanmak için gereken nitelikler ve uygunluk koşulları;

c. Her denetim makamının üye veya üyelerinin atanmasına ilişkin kurallar ve prosedürler;

d. 24 Mayıs 2016'dan sonraki ilk atama hariç, her bir denetim makamının üyesinin veya üyelerinin görev süresi dört yıldan az olmamak üzere; bunun bir kısmı bağımsızlığın korunması için gerekli olduğu durumlarda daha kısa bir süre için gerçekleşebilir. Kademeli bir atama prosedürü aracılığıyla denetim makamı;

e. Her bir denetim makamının üye veya üyelerinin kaç dönem için yeniden atanmaya uygun olup olmadığı ve eğer öyleyse, kaç dönem için uygun olduğu;

f. Her denetim makamının üye veya üyeleri ve personelinin yükümlülüklerini düzenleyen koşullar, görev süresi sırasında ve sonrasında bunlarla bağdaşmayan eylem, meslek ve menfaatlere ilişkin yasaklar ve istihdamın sona ermesini düzenleyen kurallar.

Her denetim makamının üyesi veya üyeleri ve personeli, Birlik veya Üye Devlet hukuku uyarınca, görev süreleri boyunca ve sonrasında, kendilerine ulaşan herhangi bir gizli bilgiyle ilgili olarak mesleki gizlilik yükümlülüğüne tabi olacaktır. Görevlerini yerine getirirken veya yetkilerini kullanırken edindikleri bilgilerle ilgili olarak bu mesleki gizlilik yükümlülüğü özellikle gerçek kişiler tarafından bu Tüzüğün ihlallerinin raporlanması için geçerli olacaktır.

6.5. Yetkinlik (Madde 55)

Her denetim makamı, bu Tüzük uyarınca kendisine verilen görevlerin yerine getirilmesi ve kendisine verilen yetkilerin kendi Üye Devletin topraklarında kullanılması konusunda yetkili olacaktır.

İşlemenin, 6(1) maddesinin (c) veya (e) bendi esas alınarak hareket eden kamu makamları veya özel kuruluşlar tarafından gerçekleştirildiği durumlarda, ilgili Üye Devletin denetim makamı yetkili olacaktır. Bu gibi durumlarda 56. madde uygulanmaz.

Denetleyici makamlar, adli sıfatıyla hareket eden mahkemelerin işleme faaliyetlerini denetleme yetkisine sahip değildir.

6.6. Baş Denetim Makamının Yeterliliği (Madde 56)

Kontrolörün veya işleyicinin ana kuruluşunun veya tek kuruluşunun denetim makamı, söz konusu kontrolör veya işleyici tarafından prosedüre uygun olarak gerçekleştirilen sınır ötesi işleme faaliyeti için baş denetim makamı olarak hareket etmeye yetkili olacaktır (60. madde).

Her denetim makamı, kendisine yapılan bir şikayeti veya bu Tüzük'ün olası bir ihlalinin, konunun yalnızca kendi Üye Devletindeki bir kuruluşla ilgili olması veya yalnızca kendi Üye Devletindeki veri sahiplerini önemli ölçüde etkilemesi halinde ele alma yetkisine sahip olacaktır.

Bu maddenin 2. paragrafında atıfta bulunulan durumlarda, denetim makamı, baş denetim makamını bu konu hakkında gecikmeksizin bilgilendirir.

Baş denetim makamı, bilgilendirildikten sonraki üç haftalık bir süre içinde, kontrolör veya işleyicinin bir kuruluşunun bulunup bulunmadığını dikkate alarak, davayı 60. madde uyarınca ele alıp almayacağına karar verecektir. Denetim makamının kendisini bilgilendirdiği Üye Devlet.

Baş denetim makamının davayı ele almaya karar vermesi durumunda, 60. madde sağlanan prosedür uygulanacaktır. Baş denetim makamını bilgilendiren denetim makamı, baş denetim makamına bir karar taslağı sunabilir. Baş denetim makamı, 60 (3) maddesinde atıfta bulunulan karar taslağını hazırlarken bu taslağı azami ölçüde dikkate alır.

Baş denetim makamının konuyu ele almamaya karar vermesi durumunda, baş denetim makamını bilgilendiren denetim makamı konuyu 61. ve 62. maddeler uyarınca ele alacaktır.

Baş denetim makamı, kontrolör veya işleyici tarafından gerçekleştirilen sınır ötesi işleme ilişkin tek muhatap olacaktır.

6.7. Görevler (Madde 57)

Her denetim makamı, bu Tüzük kapsamında ortaya konan diğer görevlere halel getirmeksizin, kendi topraklarında şu görevleri yerine getirecektir:

Bu Yönetmeliğin uygulanmasını izlemek ve uygulamak;

İşlemeyle ilgili riskler, kurallar, güvenceler ve haklar konusunda kamuoyunun farkındalığını ve anlayışını teşvik etmek. Özellikle çocuklara yönelik faaliyetlere özel dikkat gösterilmelidir;

Üye Devlet hukuku, ulusal parlamento, hükümet ve diğer kurum ve organlara, işlemeye ilişkin gerçek kişilerin hak ve özgürlüklerinin korunmasına ilişkin yasal ve idari tedbirler konusunda tavsiyelerde bulunmak;

Kontrolörlerin ve işleyicilerin bu Tüzük kapsamındaki yükümlülüklerine ilişkin farkındalığı teşvik etmek;

Talep üzerine herhangi bir veri sahibine bu Tüzük kapsamındaki haklarının kullanımına ilişkin bilgi sağlamak ve uygun olması halinde bu amaçla diğer Üye Devletlerdeki denetleyici makamlarla işbirliği yapmak;

madde uyarınca bir veri sahibi veya bir kurum, kuruluş veya dernek tarafından yapılan şikayetleri ele almak ve şikayetin konusunu uygun olduğu ölçüde soruşturmak ve şikayet

sahibini soruşturmanın ilerlemesi ve sonucu hakkında 80. madde uyarınca bilgilendirmek. Makul bir süre, özellikle de başka bir denetim makamıyla daha fazla soruşturma veya koordinasyonun gerekli olması halinde;

Bu Tüzüğün uygulama ve yaptırımının tutarlılığını sağlamak amacıyla diğer denetleyici makamlarla bilgi paylaşımı da dahil olmak üzere işbirliği yapmak ve karşılıklı yardım sağlamak;

Başka bir denetleyici makamından veya başka bir kamu makamından alınan bilgiler de dahil olmak üzere, bu Tüzüğün uygulanmasına ilişkin soruşturmaları yürütmek;

Kişisel verilerin korunmasına etkisi olduğu ölçüde ilgili gelişmeleri, özellikle bilgi ve iletişim teknolojilerindeki ve ticari uygulamalardaki gelişmeleri izlemek;

28(8) maddesinde ve 46 (2) maddesinin (d) bendinde atıfta bulunulan standart sözleşme maddelerini kabul etmek;

Madde 35 (4) uyarınca veri koruma etki değerlendirmesi gerekliliğine ilişkin bir liste oluşturmak ve sürdürmek;

Madde 36 (2)'de atıfta bulunulan işleme faaliyetlerine ilişkin tavsiyelerde bulunmak;

Madde 40 (1) uyarınca davranış kurallarının hazırlanmasını teşvik etmek ve Madde 40 (5) uyarınca yeterli güvenceler sağlayan bir görüş sağlamak ve bu tür davranış kurallarını onaylamak;

Madde 42 (1) uyarınca veri koruma sertifikasyon mekanizmaları ile veri koruma mühürleri ve işaretlerinin oluşturulmasını teşvik etmek ve Madde 42 (5) uyarınca sertifikasyon kriterlerini onaylamak;

Uygun olduğu durumlarda, Madde 42 (7) uyarınca verilen sertifikaların periyodik olarak gözden geçirilmesi;

Madde uyarınca davranış kurallarını izlemeye yönelik bir organın ve 43. Madde uyarınca bir sertifikasyon kuruluşunun akreditasyonu için gerekliliklerin taslağını hazırlamak ve yayınlamak;

madde uyarınca davranış kurallarını izlemeye yönelik bir organın ve 43. madde uyarınca bir sertifikasyon kuruluşunun akreditasyonunu yürütmek;

Madde 46 (3)'te atıfta bulunulan sözleşme hükümlerine ve hükümlerine yetki vermek;

Madde uyarınca bağlayıcı kurumsal kuralları onaylamak;

Kurulun faaliyetlerine katkıda bulunmak;

Bu Tüzüğün ihlallerine ve Madde 58 (2) uyarınca alınan tedbirlere ilişkin dahili kayıtları tutmak; ve

Kişisel verilerin korunmasına ilişkin diğer görevleri yerine getirmek.

Her denetim makamı, diğer iletişim araçlarını hariç tutmaksızın, elektronik olarak da doldurulabilen bir şikayet bildirim formu gibi tedbirlerle, 1. paragrafın (f) bendinde atıfta bulunulan şikayetlerin iletilmesini kolaylaştıracaktır.

Her denetim makamının görevlerinin yerine getirilmesi, veri sahibi ve uygun olduğu hallerde veri koruma görevlisi için ücretsiz olacaktır.

Taleplerin, özellikle tekrarlanan nitelikte olması nedeniyle açıkça temelsiz veya aşırı olduğu durumlarda, denetim makamı, idari maliyetlere dayalı olarak makul bir ücret talep edebilir veya talep üzerine harekete geçmeyi reddedebilir. Denetleyici makam, talebin açıkça dayanaktan yoksun veya aşırı olduğunu gösterme yükünü üstlenecektir.

6.8. Güçler (Madde 58)

Her denetim makamı aşağıdaki soruşturma yetkilerinin tümüne sahip olacaktır:

Kontrolöre, işleyiciye ve uygun olduğu durumlarda kontrolörün veya işleyicinin temsilcisine, görevlerinin yerine getirilmesi için ihtiyaç duyduğu her türlü bilgiyi sağlaması yönünde talimat verilmesi;

Veri koruma denetimleri şeklinde soruşturmalar yürütmek;

Madde 42 (7) uyarınca verilen sertifikalar üzerinde inceleme yapmak;

Kontrolöre veya işleyiciye bu Tüzüğün ihlal edildiği iddiasını bildirmek;

Kontrolörden ve işleyiciden tüm kişisel verilere ve görevlerinin yerine getirilmesi için gerekli tüm bilgilere erişim elde etmek;

Birlik veya Üye Devlet usul hukuku uyarınca, her türlü veri işleme ekipmanı ve aracı da dahil olmak üzere, kontrolör ve işleyicinin herhangi bir tesisine erişim sağlamak.

Her denetim makamı aşağıdaki düzeltme yetkilerinin tümüne sahip olacaktır:

Amaçlanan işleme operasyonlarının bu Tüzük hükümlerini ihlal etme ihtimalinin yüksek olduğu konusunda bir kontrolöre veya işleyiciye uyarılarda bulunmak;

İşleme faaliyetlerinin bu Tüzük hükümlerini ihlal ettiği durumlarda bir kontrolöre veya işleyiciye kınama cezası verilmesi;

Kontrolöre veya işleyiciye, veri sahibinin bu Yönetmelik uyarınca haklarını kullanma yönündeki taleplerine uyma talimatı verilmesi;

Kontrolöre veya işleyiciye, uygun olduğu hallerde, belirli bir şekilde ve belirli bir süre içerisinde işleme faaliyetlerini bu Tüzük hükümlerine uygun hale getirmesini emretmek;

Kontrolörün kişisel veri ihlalini veri sahibine iletmesini emretmek;

İşleme yasağı da dahil olmak üzere geçici veya kesin bir sınırlama getirmek;

16, 17 ve 18. maddeler uyarınca kişisel verilerin düzeltilmesini veya silinmesini ya da işleme faaliyetinin kısıtlanmasını emretmek ve bu tür eylemlerin 17. maddenin 2. paragrafı ve 19. madde uyarınca kişisel verilerin açıklandığı alıcılara bildirilmesini emretmek;

Bir belgeyi geri çekmek veya belgelendirme kuruluşuna 42 ve 43. maddeler uyarınca verilen bir belgeyi geri çekmesi talimatını vermek veya belgelendirme gereklilikleri yerine getirilmediği veya artık karşılanmaması durumunda belgelendirme kuruluşuna belge vermemesini emretmek;

Her bir olayın özel koşullarına bağlı olarak, bu fıkra da belirtilen tedbirlere ek olarak veya bunların yerine 83. madde uyarınca idari para cezası verilmesi;

Üçüncü bir ülkedeki alıcıya veya uluslararası bir kuruluşa veri akışının askıya alınması emrini vermek.

Her denetim makamı aşağıdaki yetki ve tavsiye yetkilerinin tümüne sahip olacaktır:

maddede atıfta bulunulan ön danışma prosedürüne uygun olarak kontrolöre tavsiyede bulunmak;

Kendi inisiyatifiyle veya talep üzerine ulusal parlamentoya, Üye Devlet hükümetine veya Üye Devlet hukuku uyarınca diğer kurum ve organların yanı sıra kamuya kişisel bilgilerin korunmasıyla ilgili herhangi bir konuda görüş bildirmek;

Üye Devletin hukukunun böyle bir ön izni gerektirmesi halinde, Madde 36 (5)'te belirtilen işleme izin vermek;

Madde 40 (5) uyarınca görüş bildirmek ve davranış kuralları taslağını onaylamak;

madde uyarınca belgelendirme kuruluşlarını akredite etmek;

Madde 42 (5) uyarınca sertifikasyonları düzenlemek ve sertifikasyon kriterlerini onaylamak;

28(8) maddesinde ve 46 (2) maddesinin (d) bendinde atıfta bulunulan standart veri koruma maddelerini kabul etmek;

46 (3) maddesinin (a) bendinde atıfta bulunulan sözleşme hükümlerine yetki vermek;

46(3) maddesinin (b) bendinde atıfta bulunulan idari düzenlemelere yetki vermek;

Madde uyarınca bağlayıcı şirket kurallarını onaylamak.

Bu Madde uyarınca denetim makamına verilen yetkilerin kullanılması, etkili hukuki çözüm ve hukuki süreç de dahil olmak üzere, Şart uyarınca Birlik ve Üye Devlet hukukunda belirtilen uygun güvencelere tabi olacaktır.

Her Üye Devlet, kendi denetim makamının, bu Tüzük ihlallerini adli makamların dikkatine sunma ve uygun olduğu hallerde, bu Tüzük hükümlerinin uygulanması amacıyla yasal işlemleri başlatma veya başka şekilde dava açma yetkisine sahip olacağını kanunla sağlayacaktır.

Her Üye Devlet, denetim makamının 1, 2 ve 3. paragraflarda atıfta bulunulan ek yetkilere sahip olmasını yasayla öngörebilir.

6.9. Etkinlik Raporları (Madde 59)

İhlal türlerinin ve alınan önlem türlerinin bir listesini içerebilecek yıllık bir rapor hazırlar .

Bu raporlar ulusal parlamentoya, hükümete ve Üye Devlet kanunları tarafından belirlenen diğer makamlara iletilecektir.

Bunlar kamunun, Komisyon'un ve Kurulun kullanımına sunulacaktır.

BÖLÜM 7. İŞBİRLİĞİ VE TUTARLILIK

7.1. Lider Denetim Makamı ile İlgili Diğer Denetim Makamları Arasında İş Birliği (Madde 60)

1. Baş denetim makamı uzlaşmaya varmak amacıyla bu madde uyarınca ilgili diğer denetim makamları ile işbirliği yapar. Baş denetim makamı ve ilgili denetim makamları ilgili tüm bilgileri birbirleriyle paylaşır.
2. Baş denetim makamı herhangi bir zamanda ilgili diğer denetim makamlarından 61. madde uyarınca karşılıklı yardım sağlamalarını talep edebilir ve özellikle soruşturmaların yürütülmesi veya başka bir üye devlette yerleşik bir kontrolör veya işleyiciye ilişkin bir tedbirin uygulanmasının izlenmesi için 62. madde uyarınca ortak operasyonlar yürütebilir.
3. Baş denetim makamı konuya ilişkin ilgili bilgileri gecikmeksizin ilgili diğer denetim makamlarına iletir. Gecikmeksizin, görüşlerini almak üzere ilgili diğer denetim makamlarına bir karar taslağı sunar ve görüşlerini gerekli şekilde dikkate alır.
4. Bu maddenin 3. paragrafı uyarınca istişarede bulunulduktan sonra dört haftalık bir süre içerisinde ilgili diğer denetim makamlarından herhangi birinin taslak karara ilişkin ilgili ve gerekçeli bir itirazda bulunması halinde, baş denetim makamı, ilgili ve gerekçeli itirazı takip etmemesi veya itirazın ilgili veya gerekçeli olmadığı kanaatinde olması halinde, konuyu 63. maddede atıfta bulunulan tutarlılık mekanizmasına sunar.
5. Baş denetim makamının yapılan ilgili ve gerekçeli itirazı takip etme niyetinde olması halinde, ilgili diğer denetim makamlarına görüşlerini almak üzere revize edilmiş bir taslak karar sunar. Bu gözden geçirilmiş taslak karar iki haftalık bir süre içerisinde 4. paragrafta atıfta bulunulan prosedüre tabi olur.
6. İlgili diğer denetim makamlarından hiçbirinin 4 ve 5. paragraflarda atıfta bulunulan süre içerisinde baş denetim makamı tarafından sunulan taslak karara itiraz etmemesi halinde, baş denetim makamı ve ilgili denetim makamlarının söz konusu taslak karar üzerinde mutabık kaldıkları kabul edilir ve bu karar ile bağlı olurlar.

7. Baş denetim makamı kararı kabul eder ve duruma göre kontrolörün veya işleyicinin ana işletmesine veya tek işletmesine tebliğ eder ve ilgili diğer denetim makamlarını ve Kurul'u ilgili olguların ve gerekçelerin bir özeti de dahil olmak üzere söz konusu karara ilişkin olarak bilgilendirir. Şikayette bulunulan denetim makamı şikayet sahibini karar hakkında bilgilendirir.
8. Bir şikayetin reddedilmesi veya reddedilmiş olması halinde, 7. paragraftan istisna olarak, şikayetin yapıldığı denetim makamı kararı kabul eder ve şikayet sahibine bildirir ve kontrolörü bu konuda bilgilendirir.
9. Baş denetim makamı ve ilgili denetim makamlarının bir şikayetin bazı kısımlarının reddedilmesi veya reddedilmesi ve söz konusu şikayetin diğer kısımlarına ilişkin olarak harekete geçilmesi hususunda mutabık kalması halinde, meselenin bu kısımlarının her biri için ayrı bir karar kabul edilir. Baş denetim makamı kontrolör ile ilgili eylemlere ilişkin kısma yönelik kararı kabul eder, kontrolör veya işleyicinin kendi üye devletin topraklarındaki ana işletmesine veya tek işletmesine bildirir ve şikayet sahibini bu konuda bilgilendirir; şikayet sahibinin denetim makamı ise söz konusu şikayetin reddedilmesi veya reddedilmesine ilişkin kısma yönelik kararı kabul eder ve bu kararı söz konusu şikayet sahibine bildirir ve kontrolör veya işleyiciyi bu konuda bilgilendirir.
10. 7 ve 9. paragraflar uyarınca baş denetim makamının kararının bildirilmesinin ardından, kontrolör veya işleyici Birlik içerisindeki tüm işletmeleri bağlamında işleme faaliyetlerine ilişkin olarak karara uyulmasını sağlamak üzere gerekli tedbirleri alır. Kontrolör veya işleyici karara uyulmasına yönelik olarak alınan tedbirleri baş denetim makamına bildirir ve bu makam da ilgili diğer denetim makamlarını bilgilendirir.
11. İstisnai durumlarda, ilgili bir denetim makamının veri sahiplerinin menfaatlerinin korunması amacıyla acil olarak harekete geçilmesi gerektiğini düşünmek için gerekçelerinin olduğu hallerde, 66. maddede atıfta bulunulan aciliyet usulü uygulanır.
12. Baş denetim makamı ve ilgili diğer denetim makamları bu madde uyarınca gereken bilgileri standartlaştırılmış bir format kullanarak elektronik yollarla birbirlerine sağlar.

7.2. Karşılıklı Yardımlaşma (Madde 61)

1. Denetim makamları bu Tüzük'ün tutarlı bir şekilde uygulanması ve yürütülmesi amacıyla birbirlerine ilgili bilgileri sağlar ve karşılıklı yardımda bulunur ve birbirleriyle etkili işbirliğine yönelik tedbirleri uygulamaya koyar. Karşılıklı yardım özellikle bilgi taleplerini ve ön izinlerin ve istişarelerin, teftişlerin ve soruşturmaların gerçekleştirilmesine yönelik talepler gibi denetim tedbirlerini kapsar.
2. Her denetim makamı başka bir denetim makamının talebine gereksiz bir gecikme olmaksızın ve talebin alınmasından sonra en geç bir ay içerisinde yanıt vermek için gereken tüm uygun tedbirleri alır. Bu tür tedbirler, özellikle, bir soruşturmanın yürütülmesine ilişkin ilgili bilgilerin iletilmesini içerebilir.
3. Yardım talepleri, talebin amacı ve nedenleri de dahil olmak üzere gerekli tüm bilgileri içerir. Değiş tokuş edilen bilgiler yalnızca talep edildiği amaç doğrultusunda kullanılır.
4. Talepte bulunulan denetim makamı aşağıdaki durumlar haricinde talebe uymayı reddedemez

- a. talebin konusu veya yerine getirmesi istenen tedbirler bakımından yetkili değildir; veya
 - b. talebin yerine getirilmesi bu Tüzük'ü veya talebi alan denetim makamının tabi olduğu Birlik ya da üye devlet hukukunu ihlal edecektir.
5. Talepte bulunulan denetim makamı talepte bulunan denetim makamını talebe yanıt vermek amacıyla alınan tedbirlerin sonuçları veya duruma göre ilerleme durumu hakkında bilgilendirir. Talepte bulunulan denetim makamı 4. paragraf uyarınca bir talebe uymayı reddetmesi halinde bunun gerekçelerini sunar.
6. Talepte bulunulan denetim makamları, kural olarak, diğer denetim makamları tarafından talep edilen bilgileri standartlaştırılmış bir format kullanarak elektronik yollarla sağlar.
7. Talepte bulunulan denetim makamları karşılıklı yardım talebi uyarınca gerçekleştirdikleri herhangi bir işlem için ücret talep etmez. Denetim makamları, istisnai durumlarda karşılıklı yardımın sağlanmasından kaynaklanan belirli harcamalar için birbirlerini tazmin etmeye yönelik kurallar üzerinde anlaşabilir.
8. Bir denetim makamının bu maddenin 5. paragrafında atıfta bulunulan bilgileri başka bir denetim makamının talebini aldıktan sonraki bir ay içerisinde sağlamaması halinde, talepte bulunan denetim makamı 55(1) maddesi uyarınca kendi üye devletinin topraklarında geçici bir tedbir kabul edebilir. Bu durumda, 66(1) maddesi kapsamındaki acil harekete geçme ihtiyacının karşılandığı varsayılır ve 66(2) maddesi uyarınca Kurul'dan acil bir bağlayıcı karar alınmasını gerektirir.
9. Komisyon, uygulama tasarrufları vasıtasıyla, bu maddede atıfta bulunulan karşılıklı yardıma ilişkin format ve usulleri ve özellikle bu maddenin 6. paragrafında atıfta bulunulan standartlaştırılmış format olmak üzere, denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin düzenlemeleri belirleyebilir. Bu uygulama tasarrufları 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

7.3. Denetim Makamlarının Ortak Operasyonları (Madde 62)

1. Denetim makamları, uygun olduğu hallerde, diğer üye devletlerin denetim makamlarının üyelerinin veya personelinin dahil olduğu ortak soruşturmalar ve ortak uygulama tedbirleri de dahil olmak üzere ortak operasyonlar yürütür.
2. Kontrolör veya işleyicinin birden fazla üye devlette işyerlerinin bulunduğu veya birden fazla üye devlette bulunan önemli sayıda veri sahibinin işleme faaliyetlerinden önemli ölçüde etkilenmesinin muhtemel olduğu hallerde, bu üye devletlerin her birinin denetim makamı ortak faaliyetlere katılma hakkına sahiptir. 256(1) veya (4) maddesi uyarınca yetkili olan denetim makamı bu üye devletlerin her birinin denetim makamını ortak operasyonlara katılmaya davet eder ve bir denetim makamının katılma talebine gecikmeksizin yanıt verir.
3. A denetim makamı, üye devlet hukuku uyarınca ve ikinci denetim makamının izniyle, ikinci denetim makamının ortak operasyonlara katılan üyelerine veya personeline soruşturma yetkileri de dahil olmak üzere yetkiler verebilir veya ev sahibi denetim makamının üye devletinin hukukunun izin verdiği ölçüde, ikinci denetim makamının üyelerinin veya personelinin soruşturma yetkilerini ikinci denetim makamının üye

devletinin hukuku uyarınca kullanmasına izin verebilir. Bu tür soruşturma yetkileri yalnızca ev sahibi denetim makamının üyeleri veya personelinin rehberliği altında ve onların huzurunda kullanılabilir. İkinci denetim makamının üyeleri veya personeli ev sahibi denetim makamının üye devlet hukukuna tabidir.

4. İkinci denetim makamının personelinin 1. paragraf uyarınca başka bir üye devlette faaliyet gösterdiği hallerde, ev sahibi denetim makamının üye devleti, topraklarında faaliyet gösterdikleri üye devletin hukuku uyarınca, faaliyetleri sırasında neden oldukları her türlü zarara ilişkin sorumluluk da dahil olmak üzere, bu kişilerin eylemlerine ilişkin sorumluluğu üstlenir.
5. Hasarın topraklarında meydana geldiği Üye Devlet, kendi personelinin neden olduğu hasara uygulanan koşullar uyarınca söz konusu hasarı telafi eder. Personeli başka bir üye devletin topraklarında herhangi bir kişiye zarar vermiş olan ikinci denetim makamının üye devleti, diğer üye devlete kendi adına hak sahibi olan kişilere ödemiş olduğu tüm meblağları tam olarak geri öder.
6. Üçüncü taraflara karşı haklarının kullanılmasına hanel gelmeksizin ve 5. paragraf istisna olmak üzere, her Üye Devlet, 1. paragrafta öngörülen durumda, 4. paragrafta atıfta bulunulan zararlar ilgili olarak başka bir Üye Devlettten geri ödeme talep etmekten kaçınır.
7. Ortak bir operasyonun amaçlandığı ve bir denetim makamının bu maddenin 2. paragrafının ikinci cümlesinde ortaya konan yükümlülüğe bir ay içerisinde uymadığı hallerde, diğer denetim makamları 55. madde uyarınca kendi üye devletin topraklarında geçici bir tedbir kabul edebilir. Bu durumda, 66(1) maddesi kapsamındaki acil harekete geçme ihtiyacının karşılandığı varsayılır ve 66(2) maddesi uyarınca Kurul'dan bir görüş veya acil bağlayıcı bir karar alınması gerekir.

7.4. Tutarlılık Mekanizması (Madde 63)

BİLGE BANK A.Ş.

Bu Tüzük'ün Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunmak amacıyla, denetim makamları bu Bölüm'de ortaya konan tutarlılık mekanizması vasıtasıyla birbirleriyle ve ilgili hallerde Komisyon ile işbirliği yapar.

7.5. Yönetim Kurulu'nun Görüşü (Madde 64)

1. Yetkili denetim makamının aşağıdaki tedbirlerden herhangi birini kabul etme niyetinde olduğu hallerde, Kurul bir görüş yayımlar. Bu amaçla, yetkili denetim makamı aşağıdaki hallerde taslak kararı Kurul'a iletir
 - a. 35(4) maddesi uyarınca bir veri koruma etki değerlendirmesi gerekliliğine tabi işleme faaliyetlerinin bir listesinin kabul edilmesinin amaçlanması
 - b. Madde 40(7) uyarınca bir taslak davranış kuralının veya bir davranış kuralında yapılan bir değişikliğin veya genişletmenin bu Tüzük ile uyumlu olup olmadığına ilişkin bir hususla ilgiliyse
 - c. Madde 41(3) uyarınca bir kuruluşun, Madde 43(3) uyarınca bir belgelendirme kuruluşunun akreditasyonu için gereklilikleri veya Madde 42(5)'te atıfta bulunulan belgelendirme kriterlerini onaylamayı amaçlar;

- d. Madde 46(2)'nin (d) bendinde ve Madde 28(8)'de atıfta bulunulan standart veri koruma hükümlerini belirlemeyi amaçlar;
 - e. 46(3) maddesinin (a) bendinde atıfta bulunulan sözleşme maddelerini yetkilendirmeyi amaçlar; veya
 - f. Madde 47 anlamında bağlayıcı kurumsal kuralları onaylamayı amaçlamaktadır.
2. Herhangi bir denetim makamı, Kurul Başkanı veya Komisyon, özellikle yetkili bir denetim makamının 61. madde uyarınca karşılıklı yardım yükümlülüklerine veya 62. madde uyarınca ortak operasyonlara ilişkin yükümlülüklere uymadığı hallerde, genel uygulamaya ilişkin veya birden fazla üye devlette etki doğuran herhangi bir hususun görüş alınması amacıyla Kurul tarafından incelenmesini talep edebilir.
 3. 1. ve 2. paragraflarda atıfta bulunulan hallerde, Kurul, aynı konuda halihazırda bir görüş vermemiş olması koşuluyla, kendisine sunulan konu hakkında bir görüş verir. Bu görüş, Kurul üyelerinin salt çoğunluğuyla sekiz hafta içinde kabul edilir. Bu süre, konunun karmaşıklığı dikkate alınarak altı hafta daha uzatılabilir. 5. paragraf uyarınca Kurul üyelerine dağıtılan 1. paragrafta atıfta bulunulan karar taslağına ilişkin olarak, Başkan tarafından belirtilen makul bir süre içerisinde itiraz etmeyen bir üye karar taslağını kabul etmiş sayılır.
 4. Denetim makamları ve Komisyon, gecikmeksizin, duruma göre olguların bir özeti, taslak karar, söz konusu tedbirin yürürlüğe konmasını gerekli kılan gerekçeler ve ilgili diğer denetim makamlarının görüşleri de dahil olmak üzere, ilgili her türlü bilgiyi standart bir format kullanarak elektronik yollarla Kurul'a iletir.
 5. Kurul Başkanı, gecikmeksizin elektronik yollarla bilgilendirme yapacaktır:
 - a. Kurul üyelerine ve Komisyon'a standart bir format kullanılarak iletilen her türlü ilgili bilgi. Kurul sekreteryası, gerektiğinde, ilgili bilgilerin tercümelerini sağlayacaktır; ve
 - b. duruma göre 1. ve 2. paragraflarda atıfta bulunulan denetim makamı ile Komisyon'a görüş bildirir ve bu görüşü kamuya açıklar.
 6. 1. paragrafta atıfta bulunulan yetkili denetim makamı 1. paragrafta atıfta bulunulan karar taslağını 3. paragrafta atıfta bulunulan süre içerisinde kabul etmez.
 7. Kurul'un görüşünü azami ölçüde dikkate alır ve görüşü almasını müteakip iki hafta içerisinde, taslak kararını muhafaza edip etmeyeceğini veya değiştirip değiştirmeyeceğini ve varsa değiştirilmiş taslak kararını standart bir format kullanarak elektronik yollarla Kurul Başkanı'na iletir.
 8. Bu maddenin 7. paragrafında atıfta bulunulan süre içerisinde, 1. paragrafta atıfta bulunulan yetkili denetim makamının ilgili gerekçeleri sunarak Kurul'un görüşünü kısmen veya tamamen takip etme niyetinde olmadığını Kurul Başkanı'na bildirmesi halinde, 65(1) maddesi uygulanır.

7.6. Uyuşmazlıkların Kurul Tarafından Çözülmesi (Madde 65)

1. Bu Tüzük'ün münferit vakalarda doğru ve tutarlı bir şekilde uygulanmasını sağlamak amacıyla, Kurul aşağıdaki durumlarda bağlayıcı bir karar kabul eder:
 - a. 60(4) maddesinde atıfta bulunulan bir durumda, ilgili bir denetim makamının baş denetim makamının bir taslak kararına yönelik ilgili ve gerekçeli bir itirazda bulunduğu ve baş denetim makamının itirazı takip etmediği veya söz konusu itirazı ilgili veya gerekçeli olmadığı gerekçesiyle reddettiği hallerde.

- Bağlayıcı karar, özellikle bu Tüzük'ün ihlal edilip edilmediği olmak üzere, ilgili ve gerekçeli itirazın konusu olan tüm hususlara ilişkindir;
- b. ilgili denetim makamlarından hangisinin ana kuruluş için yetkili olduğuna ilişkin görüş ayrılıklarının bulunduğu hallerde;
 - c. yetkili bir denetim makamının 64(1) maddesinde atıfta bulunulan hallerde Kurul'un görüşünü talep etmemesi veya 64. madde uyarınca yayımlanan Kurul görüşüne uymaması. Bu durumda, ilgili herhangi bir denetim makamı veya Komisyon konuyu Kurul'a iletebilir.
2. Paragraf 1'de atıfta bulunulan karar, konunun iletilmesinden itibaren bir ay içinde Kurul üyelerinin üçte iki çoğunluğuyla alınır. Bu süre, konunun karmaşıklığı nedeniyle bir ay daha uzatılabilir. 1. paragrafta atıfta bulunulan karar gerekçeli olur ve baş denetim makamı ile ilgili tüm denetim makamlarına gönderilir ve bu makamlar için bağlayıcıdır.
 3. Kurul'un 2. paragrafta atıfta bulunulan süreler içerisinde bir karar alamadığı hallerde, Kurul kararını 2. paragrafta atıfta bulunulan ikinci ayın sona ermesini müteakip iki hafta içerisinde Kurul üyelerinin salt çoğunluğu ile alır. Kurul üyelerinin bölünmüş olması halinde, karar Kurul başkanının oyuyla alınır.
 4. İlgili denetim makamları, 2. ve 3. paragraflarda atıfta bulunulan dönemler boyunca, 1. paragraf uyarınca Kurul'a sunulan konu hakkında bir karar kabul etmez.
 5. Kurul Başkanı, 1. paragrafta atıfta bulunulan kararı gecikmeksizin ilgili denetim makamlarına bildirir. Komisyon'u bu konuda bilgilendirir. Karar, denetim makamının 6. paragrafta atıfta bulunulan nihai kararı bildirmesinin ardından gecikmeksizin Kurul'un internet sitesinde yayımlanır.
 6. Baş denetim makamı veya, duruma göre, şikayetin yapıldığı denetim makamı, bu maddenin 1. paragrafında atıfta bulunulan karar temelinde, Kurul'un kararını bildirmesinden sonra gecikmeksizin ve en geç bir ay içerisinde nihai kararını alır. Baş denetim makamı veya, duruma göre, şikayetin yapıldığı denetim makamı, nihai kararının sırasıyla kontrolöre veya işleyiciye ve veri sahibine bildirildiği tarihi Kurul'a bildirir. İlgili denetim makamlarının nihai kararı 60(7), (8) ve (9) maddeleri hükümleri uyarınca kabul edilir. Nihai karar bu maddenin 1. paragrafında atıfta bulunulan karara atıfta bulunur ve bu paragrafta atıfta bulunulan kararın bu maddenin 5. paragrafı uyarınca Kurul'un internet sitesinde yayımlanacağını belirtir. Nihai karar, bu maddenin 1. paragrafında atıfta bulunulan kararı ekler.

7.7. Aciliyet Prosedürü (Madde 66)

1. İstisnai durumlarda, ilgili bir denetim makamının veri sahiplerinin hak ve özgürlüklerinin korunması amacıyla acil olarak harekete geçilmesi gerektiğini düşündüğü hallerde, 63, 64 ve 65. maddelerde atıfta bulunulan tutarlılık mekanizmasına veya 60. maddede atıfta bulunulan prosedüre istisna getirmek suretiyle, kendi topraklarında hukuki etkiler doğurması amaçlanan ve geçerlilik süresi üç ayı aşmayan geçici tedbirleri derhal kabul edebilir. Denetim makamı bu tedbirleri ve bunları kabul etme gerekçelerini gecikmeksizin ilgili diğer denetim makamlarına, Kurul'a ve Komisyon'a iletir.

2. Bir denetim makamının 1. paragraf uyarınca bir tedbir aldığı ve nihai tedbirlerin acilen kabul edilmesi gerektiğini düşündüğü hallerde, söz konusu denetim makamı, söz konusu görüş veya kararın talep edilmesine ilişkin gerekçeleri de belirtmek suretiyle, Kurul'dan acil bir görüş veya acil bir bağlayıcı karar talep edebilir.
3. Yetkili bir denetim makamının veri sahiplerinin hak ve özgürlüklerinin korunması amacıyla acil olarak harekete geçilmesi gereken bir durumda uygun bir tedbir almadığı hallerde, herhangi bir denetim makamı, acil olarak harekete geçilmesi gerekliliği de dahil olmak üzere, söz konusu görüş veya kararın talep edilmesine ilişkin gerekçeler sunarak, duruma göre, Kurul'dan acil bir görüş veya acil bir bağlayıcı karar talep edebilir.
4. Madde 64(3) ve Madde 65(2)'ye istisna olarak, bu maddenin 2. ve 3. paragraflarında atıfta bulunulan acil bir görüş veya acil bir bağlayıcı karar Kurul üyelerinin salt çoğunluğuyla iki hafta içerisinde alınır.

7.8. Bilgi Alışverişi (Madde 67)

Komisyon, özellikle 64. maddede atıfta bulunulan standartlaştırılmış format olmak üzere, denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin düzenlemeleri belirlemek amacıyla genel kapsamlı uygulama tasarrufları kabul edebilir.

Bu uygulama tasarrufları 93(2) maddesinde atıfta bulunulan inceleme usulüne uygun olarak kabul edilir.

7.9. Avrupa Veri Koruma Kurulu (Madde 68)

1. Avrupa Veri Koruma Kurulu ("Kurul") işbu belge ile Birliğin bir organı olarak kurulur ve tüzel kişiliğe sahip olur.
2. Kurul, Kurul Başkanı tarafından temsil edilir.
3. Kurul, her üye devletin bir denetim makamının ve Avrupa Veri Koruma Denetmeni'nin başkanı veya bunların ilgili temsilcilerinden oluşur.
4. Bir üye devlette bu Tüzük uyarınca hükümlerin uygulanmasının izlenmesinden birden fazla denetim makamının sorumlu olduğu hallerde, söz konusu üye devletin hukuku uyarınca ortak bir temsilci atanır.
5. Komisyon, oy hakkı olmaksızın Kurul'un faaliyetlerine ve toplantılarına katılma hakkına sahiptir. Komisyon bir temsilci belirler. Kurul Başkanı, Kurul'un faaliyetlerini Komisyon'a bildirir.
6. Avrupa Veri Koruma Denetmeni, 65. maddede atıfta bulunulan durumlarda, yalnızca Birlik kurumları, organları, ofisleri ve ajansları için geçerli olan ve özü itibarıyla bu Tüzük'tekilere karşılık gelen ilke ve kurallarla ilgili kararlarda oy hakkına sahiptir.

7.10. Bağımsızlık (Madde 69)

1. Kurul, 70 ve 71. maddeler uyarınca görevlerini yerine getirirken veya yetkilerini kullanırken bağımsız hareket eder.
2. Madde 70(1) ve (2)'de atıfta bulunulan Komisyon'un talepleri saklı kalmak kaydıyla, Kurul, görevlerini yerine getirirken veya yetkilerini kullanırken hiç kimseden talimat almaz veya talepte bulunmaz.

7.11. Kurulun Görevleri (Madde 70)

1. Kurul, bu Tüzüğün tutarlı bir şekilde uygulanmasını sağlar. Bu amaçla, Kurul, kendi inisiyatifiyle veya ilgili olduğu hallerde Komisyon'un talebi üzerine, özellikle
 - a. ulusal denetim makamlarının görevlerine hâlel getirmeksizin, 64 ve 65. maddelerde öngörülen durumlarda bu Tüzük'ün doğru bir şekilde uygulanmasını izler ve sağlar;
 - b. bu Tüzük'te yapılması önerilen değişiklikler de dahil olmak üzere, Birlik içerisinde kişisel verilerin korunması ile ilgili her türlü konuda Komisyon'a tavsiyelerde bulunur;
 - c. bağlayıcı kurumsal kurallar için kontrolörler, işleyiciler ve denetim makamları arasında bilgi alışverişine ilişkin format ve usuller hakkında Komisyon'a tavsiyelerde bulunur;
 - d. 17(2) maddesinde atıfta bulunulduğu üzere, kamuya açık iletişim hizmetlerinden kişisel verilerin bağlantılarının, kopyalarının veya replikalarının silinmesine yönelik usuller hakkında kılavuz ilkeler, tavsiyeler ve en iyi uygulamaları yayımlar;
 - e. kendi inisiyatifiyle, üyelerinden birinin talebi üzerine veya Komisyon'un talebi üzerine, bu Tüzüğün uygulanmasını kapsayan herhangi bir soruyu inceler ve bu Tüzüğün tutarlı bir şekilde uygulanmasını teşvik etmek amacıyla kılavuzlar, tavsiyeler ve en iyi uygulamalar yayımlar;
 - f. 22(2) maddesi uyarınca profil çıkarmaya dayalı kararlara ilişkin kriter ve koşulların daha ayrıntılı olarak belirlenmesi için bu paragrafın (e) bendi uyarınca kılavuz ilkeler, tavsiyeler ve en iyi uygulamalar yayımlar;
 - g. kişisel veri ihlallerinin tespit edilmesi ve 33(1) ve (2) maddelerinde atıfta bulunulan yersiz gecikmenin belirlenmesi ve bir kontrolör veya işleyicinin kişisel veri ihlalinin bildirmesinin gerekli olduğu belirli koşullara ilişkin olarak bu paragrafın (e) bendi uyarınca kılavuz ilkeler, tavsiyeler ve en iyi uygulamaları yayımlar;
 - h. bu paragrafın (e) bendi uyarınca, bir kişisel veri ihlalinin 34(1) maddesinde atıfta bulunulan gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riske yol açmasının muhtemel olduğu durumlara ilişkin kılavuz ilkeler, tavsiyeler ve en iyi uygulamaları yayımlar.
 - i. kontrolörler tarafından uyulan bağlayıcı kurumsal kurallara ve işleyiciler tarafından uyulan bağlayıcı kurumsal kurallara dayalı kişisel veri aktarımlarına ilişkin kriterleri ve gereklilikleri ve 47. maddede atıfta bulunulan ilgili veri sahiplerinin kişisel verilerinin korunmasını sağlamak için gerekli diğer

gereklilikleri daha fazla belirlemek amacıyla bu fıkranın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

- j. 49(1) maddesi temelinde kişisel veri aktarımlarına ilişkin kriterlerin ve gerekliliklerin daha fazla belirlenmesi amacıyla bu paragrafın (e) bendi uyarınca kılavuz ilkeler, tavsiyeler ve en iyi uygulamalar yayımlar;
- k. 58(1), (2) ve (3) maddelerinde atıfta bulunulan tedbirlerin uygulanması ve 83. madde uyarınca idari para cezalarının belirlenmesi ile ilgili olarak denetim makamları için kılavuz ilkeler hazırlar;
- l. kılavuz ilkelerin, tavsiyelerin ve en iyi uygulamaların pratikte uygulanmasını gözden geçirir;
- m. 54(2) maddesi uyarınca bu Tüzük'ün ihlallerinin gerçek kişiler tarafından bildirilmesine yönelik ortak usullerin oluşturulması için bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamalar yayımlar;
- n. 40 ve 42. maddeler uyarınca davranış kurallarının hazırlanmasını ve veri koruma belgelendirme mekanizmaları ile veri koruma mühürleri ve işaretlerinin oluşturulmasını teşvik eder
- o. 42(5) maddesi uyarınca sertifikasyon kriterlerini onaylar ve 42(8) maddesi uyarınca sertifikasyon mekanizmaları ve veri koruma mühürleri ve işaretleri ile 42(7) maddesi uyarınca üçüncü ülkelerde yerleşik sertifikalı kontrolörler veya işleyicilere ilişkin kamuya açık bir sicil tutar;
- p. Madde 43(3)'te atıfta bulunulan belgelendirme kuruluşlarının akreditasyonu amacıyla Madde 43(3)'te atıfta bulunulan gereklilikleri onaylamak
- q. Madde 43(8)'de atıfta bulunulan belgelendirme gereklilikleri hakkında Komisyon'a görüş bildirir;
- r. Madde 12(7)'de atıfta bulunulan simgeler hakkında Komisyon'a görüş bildirir;
- s. Bir üçüncü ülkenin, bir bölgenin veya söz konusu üçüncü ülkedeki bir veya daha fazla belirli sektörün veya bir uluslararası kuruluşun artık yeterli düzeyde koruma sağlayıp sağlamadığının değerlendirilmesi de dahil olmak üzere, üçüncü bir ülkedeki veya uluslararası kuruluşdaki koruma düzeyinin yeterliliğinin değerlendirilmesi için Komisyona görüş bildirir. Bu amaçla, Komisyon, söz konusu üçüncü ülke, bölge veya belirli sektör ya da uluslararası kuruluş ile ilgili olarak, üçüncü ülke hükümeti ile yapılan yazışmalar da dahil olmak üzere, gerekli tüm belgeleri Kurul'a sağlar.
- t. 64(1) maddesinde atıfta bulunulan tutarlılık mekanizması uyarınca denetim makamlarının taslak kararları hakkında, 64(2) maddesi uyarınca sunulan hususlar hakkında görüş bildirir ve 66. maddede atıfta bulunulan durumlar da dahil olmak üzere 65. madde uyarınca bağlayıcı kararlar alır;
- u. denetim makamları arasında işbirliğini ve etkili ikili ve çok taraflı bilgi ve en iyi uygulama alışverişini teşvik eder;
- v. ortak eğitim programlarını teşvik eder ve denetim makamları arasında ve uygun hallerde üçüncü ülkelerin denetim makamları veya uluslararası örgütler ile personel değişimini kolaylaştırır;
- w. dünya genelindeki veri koruma denetim makamları ile veri koruma mevzuatı ve uygulamasına ilişkin bilgi ve belge alışverişini teşvik eder.
- x. 40(9) maddesi uyarınca Birlik düzeyinde hazırlanan davranış kurallarına ilişkin görüşler yayımlar; ve

- y. tutarlılık mekanizmasında ele alınan konulara ilişkin olarak denetim makamları ve mahkemeler tarafından alınan kararların kamuya açık bir elektronik kaydını tutar.
2. Komisyon'un Kurul'dan tavsiye talep ettiği hallerde, konunun aciliyetini dikkate alarak bir süre sınırı belirtebilir.
3. Kurul görüşlerini, kılavuz ilkelerini, tavsiyelerini ve en iyi uygulamalarını Komisyon'a ve 93. maddede atıfta bulunulan komiteye iletir ve bunları kamuya açıklar.
4. Kurul, uygun olduğu hallerde, ilgili taraflara danışır ve onlara makul bir süre içinde yorum yapma fırsatı verir. Kurul, 76. maddeye hâlel getirmeksizin, istişare prosedürünün sonuçlarını kamuya açık hale getirir.

7.12. Raporlar (Madde 71)

Kurul, Birlik'te ve ilgili olduğu hallerde üçüncü ülkelerde ve uluslararası kuruluşlarda işleme faaliyetine ilişkin olarak gerçek kişilerin korunmasıyla ilgili yıllık bir rapor hazırlar. Rapor kamuya açıklanır ve Avrupa Parlamentosu'na, Konsey'e ve Komisyon'a iletilir.

Yıllık rapor, 70(1) maddesinin (l) bendinde atıfta bulunulan kılavuz ilkelerin, tavsiyelerin ve en iyi uygulamaların yanı sıra 65. maddede atıfta bulunulan bağlayıcı kararların pratikte uygulanmasına ilişkin bir incelemeyi de içerir.

BİLGE BANK A.Ş.

Korumalı İfşa Raporları

Merkez Bankası tarafından korumalı bir ifşada bulunan bir kişiden (örneğin bir muhbirden) alınan kişisel veriler de dahil olmak üzere her türlü bilgi, Merkez Bankası tarafından yasal işlevlerin yerine getirilmesi amacıyla kullanılabilir.

Merkez Bankası, yasal olarak korumalı bir ifşada bulunan bir kişinin kimliğini korumak ve belirli istisnalara tabi olarak bu kişinin kimliğini belirleyebilecek herhangi bir bilgiyi ifşa etmemekle yükümlüdür.

Merkez Bankası, muhbirler tarafından sağlanan bilgileri, ilgili herhangi bir davanın kapanmasından sonra 30 yıl süreyle saklar.

Merkez Bankası'nın muhbirler tarafından sağlanan bilgilerin nasıl ele alındığı hakkında daha fazla bilgi için bkz. Muhbirlik ve İhlal Raporları dahil Korumalı Açıklamalar

7.13. Prosedür (Madde 72)

1. Kurul, bu Tüzükte aksi belirtilmedikçe, üyelerinin salt çoğunluğuyla karar alır.

2. Kurul, üyelerinin üçte iki çoğunluğu ile kendi usul kurallarını kabul eder ve kendi operasyonel düzenlemelerini yapar.

İhaleye Katılanlar ve Mal veya Hizmet Tedarikçileri

Merkez Bankası, ihale sonuçlandırma prosedürlerini yönetmek ve belirli sözleşme yapılıp yapılmayacağına karar vermek için ihaleye katılanlar tarafından sunulan kişisel verileri işleyebilir.

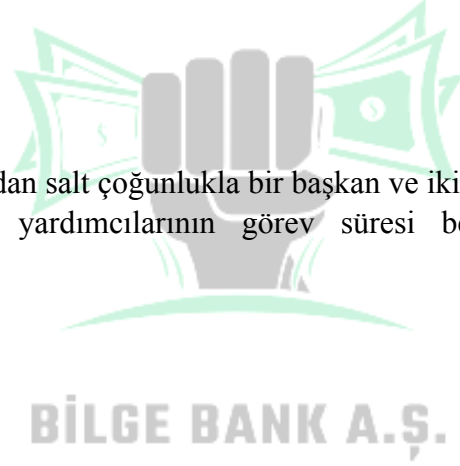
Bu amaçla toplanan kişisel veriler, ihaleye katılanlar, personeli veya alt yüklenicileri ile ilgili olabilir.

Söz konusu ihale prosedürünün sonuçlandırılması ve Merkez Bankası tarafından seçilen tedarikçi(ler) ile bir sözleşme imzalanmasının ardından, Merkez Bankası, bu sözleşme kapsamındaki yükümlülüklerin yerine getirilmesi için, örneğin ödemenin düzenlenmesi gibi, belirli kişisel verileri işleyebilir.

Satın alma prosedürlerine ilişkin dosyalar, cari yıl artı altı yıllık bir süre boyunca saklanır.

7.14. Başkan (Madde 73)

1. Kurul, üyeleri arasından salt çoğunlukla bir başkan ve iki başkan yardımcısı seçer.
2. Başkan ve başkan yardımcılarının görev süresi beş yıl olacak ve bir kez yenilenebilecektir.



7.15. Başkanın Görevleri (Madde 74)

1. Başkan aşağıdaki görevleri yerine getirecektir:
 - a. Kurul'un toplantılarını düzenlemek ve gündemini hazırlamak;
 - b. Kurul tarafından 65. madde uyarınca kabul edilen kararları baş denetim makamına ve ilgili denetim makamlarına bildirmek;
 - c. özellikle 63. maddede atıfta bulunulan tutarlılık mekanizmasına ilişkin olarak, Kurul'un görevlerinin zamanında yerine getirilmesini sağlar.
2. Kurul, usul kurallarında Başkan ve başkan yardımcıları arasındaki görev dağılımını belirler.

7.16. Sekreterlik (Madde 75)

1. Kurul, Avrupa Veri Koruma Denetmeni tarafından sağlanacak olan bir sekreteryaya sahip olacaktır.

2. Sekreteryaya, görevlerini münhasıran Kurul Başkanı'nın talimatları doğrultusunda yerine getirir.
3. Bu Tüzük ile Kurula verilen görevlerin yerine getirilmesinde yer alan Avrupa Veri Koruma Denetmeni personeli, Avrupa Veri Koruma Denetmeni'ne verilen görevlerin yerine getirilmesinde yer alan personelden ayrı raporlama hatlarına tabi olur.
4. Uygun olduğu hallerde, Kurul ve Avrupa Veri Koruma Denetmeni bu maddeyi uygulayan, aralarındaki işbirliğinin şartlarını belirleyen ve bu Tüzük ile Kurula verilen görevlerin yerine getirilmesinde yer alan Avrupa Veri Koruma Denetmeni personeli için geçerli olan bir Mutabakat Zaptı oluşturur ve yayımlar.
5. Sekreteryaya, Kurul'a analitik, idari ve lojistik destek sağlar.
6. Sekreteryaya özellikle aşağıdakilerden sorumludur
 - a. Kurul'un günlük işleri;
 - b. Kurul üyeleri, Kurul Başkanı ve Komisyon arasındaki iletişim
 - c. diğer kurumlar ve kamuoyu ile iletişim;
 - d. iç ve dış iletişim için elektronik araçların kullanımı;
 - e. ilgili bilgilerin tercüme edilmesi;
 - f. Kurul toplantılarının hazırlanması ve takibi;
 - g. görüşlerin, denetim makamları arasındaki anlaşmazlıkların çözümüne ilişkin kararların ve Kurul tarafından kabul edilen diğer metinlerin hazırlanması, kaleme alınması ve yayınlanması.

7.17. Gizlilik (Madde 76)

1. Kişisel verilerin işleme biçimi hakkında, Veri Koruma Yasaları çerçevesinde aşağıda belirtilen bir dizi hak mevcuttur:
 - a. Hakların kullanılmasıyla ilgili olarak sizden gelen herhangi bir talebe talebinizden itibaren bir ay içinde yanıt verilmesi hedeflenir, ancak bu süre bazı durumlarda Veri Koruma Yasalarına uygun olarak uzatılabilir.
 - b. Bir banka olarak, hakkında işlenen bilgilere erişme ve bu bilgilerin nereden geldiğini ve ne için kullanıldığını öğrenme hakkı bulunmaktadır.
 - c. Ayrıca, bilgilerin ne kadar süreyle saklandığı ve bilgilerin kimlerle paylaşıldığı hakkında bilgi alma hakkı da bulunmaktadır.
2. Erişim hakkı yasalar, başka bir bireyin gizliliğini koruma ihtiyacı veya bankanın ticari iş stratejileri ve operasyonları göz önünde bulundurularak kısıtlanabilir. Bu bilgileri görmek isteniyorsa bize bu adresten yazılmalıdır. Verilere erişim genellikle ücretsiz olarak sağlanır, ancak bazı durumlarda Veri Koruma Yasaları uyarınca bunu yapmaya hakkı olduğunda küçük bir ücret talep edilebilir.
3. Hakkında tutulan bilgilerin yanlış veya eksik olduğu düşünülüyorsa, bilgilerin düzeltilmesi talep edilebilir.
4. Bilgilerin kullanılmasına itiraz etme veya saklanmasına gerek yoksa silinmesi, kaldırılması veya saklamanın durdurulması talep edilebilir. Bu, 'itiraz hakkı', 'silme hakkı' veya 'unutulma hakkı' olarak bilinir. Bununla birlikte, bilgilerin saklanması veya kullanılması için yasal veya düzenleyici nedenler olabilir. Bazen bilgilerin kullanımı sadece yasal talepler veya yasal hakların kullanılması için kullanılacak şekilde kısıtlanabilir. Bu durumlarda, bilgiler kısıtlı olduğu sürece kullanılmaz veya paylaşılmaz.

5. Profil oluřturma ve otomatik karar verme. Bilge Bank, kredi veya kredi kartı bařvurularını onaylamak, dolandırıcılığı önlemek ve profil oluřturma durumunda belirli hizmetler ve ürünler sunabilmek ve genel olarak pazarlamayı hedeflemek için profil oluřturma dahil olmak üzere otomatik karar verme yöntemini kullanır. Yasal hakları etkilediđi veya üzerinde olumsuz bir etkisi olduđu durumlarda, örneđin çevrimiçi bir kredi bařvurusunun reddedilmesi gibi, otomatik karar alma sürecine tabi olmama hakkı bulunmaktadır.
6. Ayrıca, pazarlama amacıyla profil oluřturma için bilgilerin kullanılmasının durdurulması talep edilebilir. Verilerin işlenmesi için onay verildiyse ve işleme otomatikleřtirilmişse, kişisel bilgiler kolayca yeniden kullanılabilir elektronik bir formatta alınabilir. Bilgilerin bu formatta diđer kuruluşlara iletilmesi de talep edilebilir. "

Bu haklardan herhangi birini kullanmak istenirse, Veri Koruma Görevlisi ile irtibata geçilebilir;

Veri Koruma Görevlisi: Bilge Bank A.ř.

Refik Saydam Cad. No:39 řiřhane, Beyođlu – İstanbul

Veyahut kvkkbasvuru@bilgebank.com adresinden temas sađlanabilir.

BÖLÜM 8. ÇÖZÜMLER, SORUMLULUK VE CEZALAR

8.1. Bir Denetim Makamına řikayette Bulunma Hakkı (Madde 77)

Bilge Bank A.ř. olarak müşteri memnuniyetini ön planda tutuyoruz. Eğer bir müşterimiz, kişisel verilerinin işlenmesiyle ilgili olarak bu Yönetmeliđi ihlal edildiđini düşünüyorsa, ařađıdaki politikamız dođrultusunda řikayette bulunabilir:

8.1.1 řikayet Hakkı:

Her müşteri, kişisel verilerinin işlenmesine ilişkin bir ihlal olduđuna inanıyorsa, idari veya yargısal bařvuru haklarına zarar verilmemek kaydıyla, ikametgahının, işyerinin veya ihlalin gerçekte olduđu yerin bulunduđu Üye Devlet'teki denetim otoritesine řikayette bulunma hakkına sahiptir.

8.1.2. Bilgilendirme ve İlerleme:

řikayetin yapıldıđı denetim otoritesi, řikayetçiye řikayetin gelişimi ve sonucu hakkında düzenli olarak bilgilendirecek ve aynı zamanda yargı yolu olup olmadığı konusunda müşteriyi bilgilendirecektir.

8.2. Denetim Makamına Karşı Etkili Bir Yargı Yoluna Bařvurma Hakkı (Madde 78)

Bilge Bank A.ř. olarak müşteri memnuniyetini ve řeffaflıđı ön planda tutuyoruz. Herhangi bir müşteri, denetim otoritesinin kendisi hakkında bađlayıcı bir kararı olduđunda, ařađıdaki politikamız çerçevesinde etkili bir yargı yoluna bařvurabilir:

8.2.1. Yargı Yolu Hakkı:

Her müşteri, kendisi hakkında bir denetim otoritesinin bağlayıcı bir kararı olduğu takdirde, idari veya yargı dışı başka bir çözüm hakkına zarar gelmeksizin etkili bir yargı yoluna başvurma hakkına sahiptir.

Bilge Bank A.Ş. olarak, müşteri memnuniyetini ve veri sahiplerinin haklarını koruma konusunu ön planda tutuyoruz. Herhangi bir müşteri, denetim otoritesinin bir şikayeti ele almaması veya yapılan şikayetin ilerlemesi veya sonucu hakkında üç ay içinde bilgi vermemesi durumunda, idari veya yargı dışı başka bir çözüm hakkına zarar gelmeksizin etkili bir yargı yoluna başvurabilir.

Denetim otoritesine karşı başlatılacak yargı süreci, denetim otoritesinin bulunduğu Üye Devlet'in mahkemeleri önünde yapılır.

Denetim otoritesinin bir tutarlılık mekanizması kapsamında alınan bir görüş veya karardan önce verilen bir kararın ardından yapılan bir kararın hukuki süreçlere taşınması durumunda, denetim otoritesi, bu görüşü veya kararı mahkemeye iletacaktır.

8.3. Bir Kontrolör veya İşleyiciye Karşı Etkili Bir Yargı Yoluna Başvurma Hakkı (Madde 79)

Bilge Bank A.Ş. olarak müşteri memnuniyetini ve veri sahiplerinin haklarını ön planda tutuyoruz. Herhangi bir müşteri, kişisel verilerinin bu Yönetmelik'e uygun olmayan bir şekilde işlenmesi sonucunda bu Yönetmelik kapsamındaki haklarının ihlal edildiğini düşünüyorsa, idari veya yargı dışı başka bir çözüm hakkına zarar gelmeksizin etkili bir yargı yolu hakkına başvurabilir.

Bir kontrolör veya işleyiciye karşı başlatılacak yargı süreci, kontrolörün veya işleyicinin bir tesisinin bulunduğu Üye Devlet'in mahkemeleri önünde yapılır.

Alternatif olarak, bu tür süreçler, kontrolör veya işleyici bir Üye Devlet'in kamu yetkilerini kullanarak hareket eden bir kamu otoritesi değilse, veri sahibinin ikametgahının bulunduğu Üye Devlet'in mahkemeleri önünde de başlatılabilir.

8.4. Veri Sahiplerinin Beyanı (Madde 80)

1. Veri sahibi, bir Üye Devletin hukukuna uygun şekilde oluşturulmuş, kamu yararına olan yasal hedefleri bulunan ve kişisel verilerinin korunmasına ilişkin olarak veri sahiplerinin hak ve özgürlüklerinin korunması alanında faaliyet gösteren kar amacı gütmeyen bir organ, kuruluş veya derneği kendi adına şikayette bulunmak, 77, 78 ve 79. maddelerde atıfta bulunulan hakları kendi adına kullanmak ve Üye Devlet hukuku tarafından öngörüldüğü hallerde 82. maddede atıfta bulunulan tazminat alma hakkını kendi adına kullanmak üzere yetkilendirme hakkına sahiptir.

2. Üye devletler, bu maddenin 1. paragrafında atıfta bulunulan herhangi bir organ, kuruluş veya birliğin, bir veri sahibinin yetkisinden bağımsız olarak, söz konusu üye devlette 77. madde uyarınca yetkili olan denetim makamına şikayette bulunma ve bir veri sahibinin bu Tüzük kapsamındaki haklarının işleme faaliyeti sonucunda ihlal edildiğini düşünmesi halinde 78 ve 79. maddelerde atıfta bulunulan hakları kullanma hakkına sahip olmasını sağlayabilir.

8.5. İşlemlerin Askıya Alınması (Madde 81)

1. Bir üye devletin yetkili mahkemesinin aynı kontrolör veya işleyici tarafından gerçekleştirilen işleme faaliyetlerine ilişkin aynı konu hakkında başka bir üye devletteki bir mahkemede derdest olan yargılamalar hakkında bilgi sahibi olması halinde, söz konusu yargılamaların varlığını teyit etmek üzere diğer üye devletteki mahkeme ile temasa geçer.
2. Aynı kontrolör veya işleyicinin işleme faaliyetine ilişkin aynı konu hakkındaki yargılamaların başka bir üye devletteki bir mahkemede derdest olduğu hallerde, ilk el koyan mahkeme dışındaki herhangi bir yetkili mahkeme yargılamaları askıya alabilir.
3. Bu yargılamaların ilk derece mahkemesinde derdest olduğu hallerde, ilk derece mahkemesinin söz konusu davalar üzerinde yargı yetkisine sahip olması ve hukukunun bunların birleştirilmesine izin vermesi halinde, ilk derece mahkemesi dışındaki herhangi bir mahkeme de taraflardan birinin başvurusu üzerine yargı yetkisini reddedebilir.

8.6. Tazminat Hakkı ve Sorumluluk (Madde 82)

8.6.1. Tazminat Hakkı Genel İlkeler:

GDPR kapsamında, hak ihlaline (hukuka aykırı işleme, veri sızıntısı gibi hallerde) uğrayan veri sahiplerine tazminat talebi imkanı tanınmıştır. Bu hak, veri sahiplerine, kişisel verilerinin hukuka aykırı bir şekilde işlenmesi nedeniyle doğan maddi veya manevi zararlarının telafi edilmesi amacını taşır.

8.6.2. Tazminat Talebi İçin Şartlar:

Veri sahipleri, tazminat talebinde bulunabilmek için aşağıdaki şartların varlığını göstermelidir:

a. Hak İhlali:

Tazminat talebi, kişisel verilerin hukuka aykırı bir şekilde işlenmesi, yetkisiz erişim, veri sızıntısı veya başka bir hak ihlali durumunda geçerlidir.

b. Zarar:

Talep edilen tazminatın temeli, veri sahibinin maruz kaldığı zarara dayanmalıdır. Zarar, maddi veya manevi olabilir ve hak ihlalinin doğrudan bir sonucu olmalıdır.

c. İhlalin Tescili:

Veri sahibi, hak ihlalinin varlığını tespit etmiş ve kayıt altına almış olmalıdır. Bu, veri sahibinin ihlali fark etmesi ve ilgili olayları belgelemesi anlamına gelir.

8.6.3. İlgili Tarafların Hakları:

Tazminat talebinde bulunan veri sahibi, talebinin ilgili veri sorumlusu tarafından değerlendirilmesi ve cevaplanması hakkına sahiptir. İlgili taraflar, talep sürecinde adil bir şekilde bilgilendirilir ve sürecin şeffaf bir şekilde yürütülmesi sağlanır.

8.6.4. Uyuşmazlık Çözümü:

Tazminat talepleri, mümkünse taraflar arasında uzlaşma yoluyla çözülmeye çalışılır. Ancak taraflar arasında uzlaşma sağlanamazsa, veri sahibi hukuki yollara başvurabilir ve yetkili mahkemede tazminat davası açabilir.

Bu madde, GDPR kapsamında veri sahiplerine tanınan tazminat hakkını detaylandırarak, hak ihlali durumunda veri sahiplerinin tazminat talebinde bulunma süreçlerini ve şartlarını açıklamaktadır.

8.7. İdari Para Cezalarının Uygulanmasına İlişkin Genel Koşullar (Madde 83)

İdari para cezası verilirken verilmeyeceğine ve her bir olay için idari para cezasının miktarına karar verilirken aşağıdaki hususlar dikkate alınacaktır:

- İlgili işleme faaliyetinin niteliği, kapsamı ve amacı ile etkilenen veri sahiplerinin sayısı ve uğradıkları zarar düzeyi dikkate alınarak ihlalin niteliği, ciddiyeti ve süresi;
- İhlalin kasıtlı veya ihmalkar niteliği;
- Veri sahiplerinin maruz kaldığı zararı hafifletmek için kontrolör veya işleyici tarafından gerçekleştirilen herhangi bir işlem;
- Kontrolör veya işleyici tarafından daha önce yapılmış ilgili ihlaller;
- İhlalin giderilmesi ve ihlalin olası olumsuz etkilerinin hafifletilmesi amacıyla denetim makamıyla işbirliğinin derecesi;
- İhlalden etkilenen kişisel veri kategorileri;
- İhlalin denetim makamına nasıl bildirildiği ve özellikle kontrolör veya işleyicinin ihlali bildirip bildirmediği ve bildirmişse ne ölçüde;
- İhlalden doğrudan veya dolaylı olarak elde edilen mali faydalar veya kaçınılan kayıplar gibi, davanın koşullarına uygun diğer ağırlaştırıcı veya hafifletici faktörler.

Eğer bir kontrolör veya işleyici, aynı veya bağlantılı işlemler için bu Tüzük'ün birkaç hükmünü kasıtlı olarak veya ihmal sonucu ihlal ederse, idari para cezasının toplam miktarı, en ciddi ihlal için belirlenen miktarı aşmamalıdır. Aşağıdaki hükümlerin ihlalleri,

2. paragrafa göre, idari para cezalarına 10.000.000 EUR'a kadar veya bir işletme ise önceki mali yılın toplam dünya genelindeki yıllık cirosunun %2'sine kadar, hangisi daha yüksekse, tabi olacaktır:

- Kontrolör ve işleyiciye ait yükümlülükler
- Sertifikasyon kuruluşuna ait yükümlülükler
- Ait yükümlülükler

Denetim otoritesi tarafından verilen bir emre uymamanın, bu maddeye göre 2. paragrafa göre, idari para cezalarına tabi olması 20.000.000 EUR'a kadar veya bir işletme ise önceki mali yılın toplam dünya genelindeki yıllık cirosunun %4'üne kadar, hangisi daha yüksekse.

Denetim otoritelerinin düzeltici yetkilerinden bağımsız olarak, her Üye Devlet, o Üye Devlet'te kurulu kamu otoriteleri ve kuruluşları üzerinde idari para cezalarının hangi durumda ve ne ölçüde uygulanabileceğine dair kuralları belirleyebilir.

Denetim otoritesinin bu madde kapsamındaki yetkilerini kullanması, Birlik ve Üye Devlet hukukuna uygun olarak uygun prosedür güvencelerine tabi olacaktır, bunlar arasında etkili yargı yolunu ve hukuki süreci içerir.

Üye Devletin hukuki sistemi idari para cezalarını öngörmüyorsa, bu madde, yetkili denetim otoritesi tarafından başlatılan ve yetkili ulusal mahkemeler tarafından uygulanan bir para cezası yöntemiyle uygulanabilir. Bu süreç, bu hukuki başvuruların etkili olduğunu ve denetim otoriteleri tarafından uygulanan idari para cezalarına eşit etkiye sahip olduğunu sağlamak koşuluyla gerçekleştirilir. Her durumda, uygulanan para cezaları etkili, orantılı ve caydırıcı olmalıdır.

8.8. Cezalar (Madde 84)

1. Üye Devletler, özellikle 83. madde uyarınca idari para cezalarına tabi olmayan ihlaller için olmak üzere, bu Tüzüğün ihlallerine uygulanacak diğer cezalara ilişkin kuralları belirler ve bunların uygulanmasını sağlamak için gerekli tüm tedbirleri alır. Bu tür cezalar etkili, orantılı ve caydırıcı olmalıdır.
2. Her Üye Devlet, 1. paragraf uyarınca kabul ettiği mevzuat hükümlerini 25 Mayıs 2018 tarihine kadar ve bunları etkileyen müteakip değişiklikleri de gecikmeksizin Komisyon'a bildirir.



BÖLÜM 9. BELİRLİ İŞLEME DURUMLARI İLE İLGİLİ HÜKÜMLER

9.1. İşleme ve İfade ve Bilgi Edinme Özgürlüğü (Madde 85)

Üye devletler, ifade ve bilgi edinme özgürlüğü hakkının korunmasıyla birlikte gazetecilik, akademik, sanatsal veya edebi ifade amaçları için kişisel verilerin işlenmesi hakkını da kanunla bağdaştırmaktadır. Eğer gazetecilik veya akademik, sanatsal veya edebi ifade amaçlarına yönelik işleme faaliyetleri gerçekleştiriliyorsa, üye devletler, bu durumu kişisel verilerin korunması hakkıyla bağdaştırmak için gerekli olan muafiyetler veya istisnalar sağlar. Bu istisnalar veya muafiyetler, belirli veri işleme durumları, veri sahibinin hakları, veri kontrolü ve işleme, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması, bağımsız denetim makamları, işbirliği ve tutarlılık gibi bölümleri içeren Tüzük'ün ilgili hükümlerinden kaynaklanır. Her üye devlet, kabul ettiği yasanın hükümlerini ve bu hükümleri etkileyen değişiklikleri Komisyon'a zamanında bildirir.

9.2. Resmi Belgelerin İşlenmesi ve Kamuya Açık Erişim (Madde 86)

Kamu yararına yürütülen bir görevin yerine getirilmesi amacıyla bir kamu makamı veya kamu kurumu veya özel bir kuruluş tarafından tutulan resmi belgelerde yer alan kişisel veriler, kamunun tabi olduğu Birlik veya Üye Devlet hukukuna uygun olarak yetkili makam

veya kuruluş tarafından açıklanabilir. Kamunun resmi belgelere erişimini, bu Yönetmelik uyarınca kişisel verilerin korunması hakkıyla bağdaştırmak için yetkili makam veya organ tabidir.

9.3. Ulusal Kimlik Numarasının İşlenmesi (Madde 87)

Üye Devletler ayrıca ulusal kimlik numarasının veya genel uygulamaya yönelik diğer herhangi bir tanımlayıcının işlenmesine ilişkin özel koşulları belirleyebilir. Bu durumda, ulusal kimlik numarası veya genel uygulamaya yönelik diğer herhangi bir tanımlayıcı, yalnızca bu Tüzük uyarınca veri sahibinin hakları ve özgürlüklerine yönelik uygun güvenceler kapsamında kullanılacaktır.

9.4. İstihdam Bağlamında İşleme (Madde 88)

Üye devletler, işverenlerin çalışanların kişisel verilerini işleme konusunda belirli kurallar öngörebilirler. Bu kurallar işe alım, iş sözleşmesinin yerine getirilmesi ve yasal yükümlülüklerin yerine getirilmesi gibi konuları kapsayabilir. Ayrıca, iş yönetimi, eşitlik ve çeşitlilik, sağlık ve güvenlik, mülkiyet korunması, işle ilgili hakların bireysel veya toplu kullanımı gibi konularda da kurallar belirlenebilir. Veri sahibinin insan onurunu, meşru menfaatlerini ve temel haklarını korumak için şeffaflık, veri aktarımı ve izleme sistemleri gibi konularda özel tedbirler alınması gerekmektedir.

9.5. Kamu Çıkarına Yönelik Arşivleme Amaçları, Bilimsel veya Tarihi Araştırma Amaçları veya İstatistiksel Amaçlarla İşlemeye İlişkin Güvenceler ve İstisnalar (Madde 89)

Kişisel verilerin belirli amaçlar doğrultusunda işlenmesi durumunda hangi koşulların ve güvencelerin geçerli olacağı belirtilmektedir. Bu amaçlar, kamu yararına arşivleme, bilimsel veya tarihi araştırma veya istatistiksel amaçlar olarak sınıflandırılmaktadır. Veri sahibinin haklarını ve özgürlüklerini korumak amacıyla, teknik ve organizasyonel tedbirler alınması gerekmektedir. Bu tedbirler, veri minimizasyonu ilkesine uyulmasını sağlamayı amaçlamaktadır. Ayrıca, takma ad kullanma gibi önlemler de alınabilir. Veri sahiplerinin kimliklerinin belirlenebildiği durumlarda, bu amaçlar bu şekilde gerçekleştirilebilir. Bilimsel veya tarihi araştırma veya istatistiksel amaçlar için yapılan veri işleme faaliyetlerinde, belirli amaçların gerçekleştirilmesini imkansız hale getirme veya ciddi şekilde zarar verme durumunda, istisnalar getirilebilir. Benzer şekilde, kamu yararına arşivleme amacıyla yapılan veri işleme faaliyetlerinde de, istisnalar uygulanabilir. Bu istisnaların koşullara ve güvencelere tabi olması gerekmektedir.

9.6. Gizlilik Y k ml l kleri (Madde 90)

Kişisel verilerin korunması hakkı ile gizlilik y k ml l ğ  arasında bir denge saėlamak amacıyla  ye devletlerin kontrol rler veya iřleyiciler i in kurallar belirleyebileceėi belirtilmektedir. Bu kurallar, 58(1) maddesinin (e) ve (f) bentlerinde belirtilen denetim makamlarının yetkilerini saptamak amacıyla Birlik veya  ye devlet hukuku veya ulusal yetkili organlar tarafından oluřturulabilir. S z konusu kurallar, kontrol r veya iřleyicinin kiřisel verilerle ilgili gizlilik y k ml l ğ   er evesinde yaptėėı faaliyetlerle ilgili olarak uygulanır.

