

KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

1. GİRİŞ

Ülkemizde başta özel hayatın gizliliğinin korunması olmak üzere temel hak ve özgürlükler, Türkiye Cumhuriyeti Anayasası ile güvence altına alınmıştır. 2010 yılında Anayasa'nın 20. maddesine bu kapsamda eklenen bir fıkra ile kişisel verilerin işlenmesi hakkında bilgilendirilme, bu verilere erişim sağlayabilme, düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme, temel bir hak olarak tanımlanmıştır. Kişisel verilerin saklanması, işlenmesi, üçüncü taraflara aktarılması ve imhasına ilişkin usul ve esaslar ile tarafların hak ve yükümlülükleri ise 07.04.2016 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu ile düzenlenmiştir.

Türkiye İş Bankası A.Ş., “veri sorumlusu” sıfatıyla uhdesindeki her türlü kişisel veriyi bu Kanun ve sair mevzuat kapsamında korumak için uygun güvenlik düzeyini temin etmek amacıyla gerekli idari ve teknik tedbirleri almaktan, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemekten sorumludur.

Banka, bu sorumluluklarını Kişisel Verilerin Korunması Kanunu ve bu Kanuna dayalı ikincil düzenlemelerin gerekliliklerini, Kişisel Verileri Koruma Kurulu ve mahkeme kararlarını ve sair mevzuatı göz önüne alarak yerine getirir.

2. AMAÇ

Kişisel Verilerin Korunması Politikası'nın amacı, Banka tarafından gerçekleştirilen veri işleme faaliyetlerinin başta Anayasa ve Kişisel Verilerin Korunması Kanunu olmak üzere yasal düzenlemelere uyumlu olarak yürütülmesini, kişisel verilerin işlenmesini süreç ve faaliyetlerinin bu Politikada tanımlanan ilke, usul ve esaslar çerçevesinde sürdürülmesini sağlamaktır. Bu bağlamda, tüm faaliyetlerin bu esaslar ile bilgi güvenliğinin sağlanmasına yönelik diğer dâhili düzenlemeler doğrultusunda sürdürülmektedir.

3. KAPSAM

Politika; Türkiye İş Bankası A.Ş. Mensupları Emekli Sandığı Vakfı emeklileri ve çalışanları, Türkiye İş Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Sandığı Vakfı emeklileri ve çalışanları ile Türkiye İş Bankası kadrosunda yer alıp Banka iştiraklerinde çalışanları ve sair gerçek kişi gruplarının otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla Banka tarafından işlenen tüm kişisel verilerinin korunmasına ilişkindir.

Kanun çerçevesinde temel olarak, “verileri işlenen gerçek kişiler” koruma altına alınmakla birlikte, “bir gerçek kişinin belirlenmesini sağlayan” tüzel kişiye ait veriler de Kanun'un, dolayısıyla Politika'nın kapsamında yer almaktadır.

4. TANIMLAR

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza,

Banka: Türkiye İş Bankası A.Ş.,

İlgili Kişi: Kişisel verisi işlenen gerçek kişi,

Kanun: Kişisel Verilerin Korunması Kanunu,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi,

Kişisel Verilerin İşlenmesi; 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,

Politika: İşbu Kişisel Verilerin Korunması Politikası,

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi,

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi ve

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi (bu Politika çerçevesinde Türkiye İş Bankası A.Ş.) anlamına gelmektedir.

5. TEMEL ESASLAR

5.1. Genel İlkeler

Banka, uhdesinde bulunan veya toplayacağı kişisel verileri;

- hukuka ve dürüstlük kurallarına uygun olarak,
- doğru ve güncel olması için gerekli ve yeterli çabayı göstererek,
- belirli, açık ve meşru amaçlarla,
- işleme amacı ile bağlantılı, sınırlı ve ölçülü olarak ve
- ilgili mevzuatta öngörülen veya işleme amacının gerektirdiği süre kadar muhafaza ederek işler.

5.2. Aydınlatma Yükümlülüğü

Banka, kişisel verisini işleyeceği ilgili kişileri aydınlatmakla yükümlüdür. Söz konusu yükümlülük çerçevesinde Banka, kişisel verilerin elde edilmesi sırasında ilgili kişiyi;

- Bankanın kimliği (Türk Ticaret Kanununun 1524. maddesi ile düzenlenen ve Banka internet sitesinde yayınlanan tanıtıcı bilgiler),
- kişisel verinin işleme amacı,
- işlenen kişisel verinin kimlere hangi amaçla aktarılabilceği,
- kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Politikanın 7. maddesinde belirtilen ilgili kişinin hakları konularında bilgilendirecektir. Banka, bu sorumluluğunu şubeleri, interaktif kanalları ve muhtelif ilgili kişi grupları açısından idari olarak uygun görülen diğer araç ve yöntemler ile yerine getirir.

5.3. Kişisel Verilerin İşlenme Şartları

Aktarılan prensipler doğrultusunda kişisel veriler, aşağıda belirtilen şartların varlığı dışında kişinin bu yönde açık rızası olmaksızın işlenemez.

Kişisel veriler;

- kanunlarda açıkça öngörülmesi,

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

durumlarından birinin varlığı halinde ilgili kişinin rızası aranmaksızın işlenebilir. İşleme amacı ortadan kalkan veriler, Kişisel Veri Saklama ve İmha Politikası ile belirlenen esaslara uygun olarak imha edilir.

Banka, kişisel verileri yalnızca ilgili kişinin özgür iradesi ile beyan ettiği açık rızasının bulunması ya da yukarıda değinilen işleme şartlarının mevcudiyeti halinde işler. Veri sorumlusu olarak Bankanın ispat yükümlülüğünün yerine getirilmesini teminen kişilerin açık rıza tercihleri kimlik tespiti yapılabilen veya kimlik doğrulaması gerçekleştirilebilen kanallar üzerinden alınır.

Politika, Banka'nın kişisel verilerin işlenmesi faaliyetlerinin tamamını kapsamakta olup, gereklerine tüm Banka çalışanları ve ilgili 3. taraflarca uyulması zorunludur.

5.4. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Kanunda “özel nitelikli kişisel veri” olarak tanımlanan, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler, Kanun 6/3. maddesinde belirtilen açık rıza veya diğer şartların mevcudiyeti halinde işlenebilmektedir.

Banka, özel nitelikli kişisel verilerin korunması amacıyla konuya özel bir politikayı ilgili mevzuatta belirtilen gerekli önlemleri içerecek şekilde oluşturur ve uygulanmasını sağlar.

5.5. Kişisel Verilerin Aktarımı

Banka, kişisel verilerin yurt içinde veya yurt dışındaki kişi ve kuruluşlara aktarımı konusunda Kanunun ve sair diğer mevzuatın gerekliliklerini yerine getirerek hareket eder.

Kişisel verilerin yurt dışına aktarımı, ilgili kişinin bu yönde açık rızası bulunması koşuluna bağlanmışsa da kişisel veriler, Politika'nın 6.3 ve 6.4. maddelerinde belirtilen işleme şartlarına ek olarak Kanun'da belirtilen şartının sağlanması koşuluyla yurt dışına aktarılabilir.

Kişisel verilerin yurt içinde ve yurt dışına aktarımında diğer kanunlarda yer alan hükümler saklıdır.

5.6. İlgili Kişinin Hakları

İlgili kişiler, Banka'ya başvurarak kendileri ile ilgili;

- kişisel verilerinin işlenip işlenmediğini öğrenme,
- kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme,

- kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kanun'un 7. maddesinde düzenlenen şartlar dâhilinde kişisel verilerinin silinmesini veya yok edilmesini isteme,
- yapılan düzeltme, silme ve yok etme işlemlerinin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- işlenen verilerinin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

haklarına sahiptir. İlgili kişi taleplerinin Banka tarafından değerlendirilebilmesi için kimlik tespit yükümlülüğünün yerine getirilmesi ve işlem güvenliğinin sağlanması gerekmektedir. Bu çerçevede, ilgili kişi başvuruları;

- Şubelerimizde kimlik belgesi kontrolü ve kimlik tespiti yapılmasının ardından ilgili kişinin ıslak imzasını taşıyan talep yazısı alınarak,
- kimlik doğrulaması yapılabilen dijital kanallar üzerinden,
- noter kanalıyla "İş Kuleleri 34330 Levent Beşiktaş-İstanbul" adresine gönderilerek,
- isbankasi@hs02.kep.tr adresine güvenli elektronik imzalı olarak iletilerek

Banka'ya aktarılmalıdır. Bankaya daha önce bildirilen ve Banka sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle de ilgili kişi başvuruları iletilebilecek olmakla birlikte; bu yöntemin kullanılması durumunda ilgili kişi kimlik tespiti ya da doğrulaması imkânı bulunan diğer kanallara yönlendirilecektir.

Banka, ilgili kişi taleplerini kabul eder veya gerekçesini açıklayarak reddeder; konuya ilişkin yanıtı ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. İlgili kişi taleplerinin en kısa sürede ve en geç 30 gün içinde sonuçlandırılması gereği Kanun ile düzenlenmiştir.

5.7. Veri Sorumlusunun Veri Güvenliğine İlişkin Yükümlülükleri

Banka, veri sorumlusu olarak uhdesinde bulunan kişisel verilerin güvenliği konusunda Kanun ile yükümlü tutulmuştur. Veri sorumlusu, kişisel verilere hukuka aykırı olarak erişilmesini ve hukuka aykırı veri işlenmesini engellemekle yükümlü olup, kişisel verilerin güvenli bir şekilde muhafaza edilmesi için gerekli tüm teknik ve idari tedbirleri almakla ve gerekli denetimleri yapmak veya yaptırmakla yükümlüdür. Banka söz konusu yükümlülüğü yerine getirirken temel bilgi güvenliği prensiplerinin Banka genelinde uygulanmasını sağlamak amacıyla gerekli politika ve standartları oluşturur, bunlara yönelik farkındalık araçları geliştirir ve tüm paydaşların hassasiyetlerinin üst seviyede tutulması amacıyla uygun kanalları kullanarak sürekli bir iletişim sağlar.

Banka, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır ve denetim sonuçları doğrultusunda gerekli aksiyonları alır.

Bankanın veri sorumlusu olduğu kişisel verilerin bir veri işleyen vasıtasıyla işlenmesi halinde, Kanun, meydana gelebilecek zararlardan hem Bankayı hem de veri işleyeni müştereken sorumlu tutmaktadır. Bu nedenle kişisel verilerin veri işleyenlere aktarılmasında hem sözleşme kapsamında hem de teknik ve idari olarak tüm tedbirler alınır ve veri işleyenlerden de Kanun ve sözleşme ile öngörülen tüm yükümlülükleri yerine getirmeleri talep edilir. Bu çerçevede, veri işleyen üçüncü taraflar ile Banka arasında düzenlenecek sözleşmelerde kişisel verilerin korunmasına, işlenmesine, saklanmasına veya ilgili kişinin talebi ya da işleme amacının ortadan kalkması gibi nedenlerle yok edilmesine yönelik asgari

güvenlik standartlarının belirtilmesi ve iş ilişkisinin sürdüğü süre zarfında sürecin söz konusu standartlara uyum durumu Banka tarafından takip edilmektedir. Bu çerçevede, veri işleyen üçüncü tarafların Bankanın kendi denetim birimlerince ya da Bankanın talebi doğrultusunda dış denetçiler tarafından denetlenebileceğine dair gerekli hükümler sözleşmelere eklenir.

Kanun ayrıca kişisel veriler ile Banka bünyesinde ya da Bankanın görevlendirmesi ile çalışan gerçek kişilere de sorumluluk yüklemektedir. Kanuna göre bu kişiler söz konusu kişisel verileri Kanun hükümlerine aykırı olarak başkalarına açıklayamaz ve işleme amacı dışında kullanamazlar. Görevden ayrılmış olsalar dahi bu konudaki sorumlulukları hukuken devam eder. Bu nedenle tüm Banka çalışanları kişisel verilerin korunmasından hem müşterek olarak hem de bireysel olarak sorumludurlar.

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi durumunda Banka bu durumu en kısa sürede ilgili kişiye ve Kurul tarafından belirlenecek usullere uygun olarak Kurula bildirir.

Banka, veri sorumlusu olması itibarıyla, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından kamuya açık olarak tutulacak olan “Veri Sorumluları Sicili”ne kaydolmak zorundadır. Banka bu yükümlülüğünü Veri Sorumluları Sicili Hakkında Yönetmelik hükümleri ve Kurulca belirlenecek diğer usul ve esaslar doğrultusunda yürütür.

6. Kişisel Veri İhlal Olayı Tanımı ve Referans

Kişisel Verilerin Korunması Kanunu, kişisel veri ihlaline ilişkin bir tanım öngörmemekle birlikte; kişisel verilerin “kanuni olmayan yollarla başkaları tarafından elde edilmesi” durumu kişisel veri ihlali olarak değerlendirilmektedir.

Kişisel Veri İhlal Olayı Yönetimi Standardı, Kişisel Verilerin Korunması Politikasında belirtilen esaslar çerçevesinde oluşturulmuştur ve anılan politikanın ayrılmaz bir parçasıdır.

6.1 Kişisel Veri İhlal Olaylarının Bildirimi

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi durumunda Banka bu durumu en kısa sürede ilgili kişiye ve Kurul tarafından belirlenecek usullere uygun olarak Kurula bildirir.

Bildirimler kişisel veri ihlalinin öğrenildiği tarihten itibaren en geç 72 saat içerisinde mevzuatta belirlenen esaslar çerçevesinde gerçekleştirilir. Söz konusu veri ihlalden etkilenen ilgili kişilere de makul olan en kısa süre içerisinde bildirimde bulunulur.

7. GÖZETİM/DENETİM

İş süreçlerinin Politika esasları çerçevesinde tasarlanması ve buna uygun şekilde işletilmesinin sağlanması, Banka’nın sorumluluğundadır. Banka, bu politika hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

Kişisel verilerin saklanması, işlenmesi, üçüncü taraflara aktarılması ve imhasına ilişkin usul ve esaslar ile tarafların hak ve yükümlülükleri 07.04.2016 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ile düzenlenmiştir.

Kişisel verilerin ilgili tüm kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından imha edilmesi gereğine Kanunda yer verilmiştir.

Bu politika, Türkiye İş Bankası A.Ş. Kişisel Verilerin Korunması Politikası'nın ayrılmaz bir parçasıdır.

2. AMAÇ

Bu politikanın amacı, Kanun'a dayalı olarak 28.10.2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (Yönetmelik) gereği kişisel verilerin saklanması ve imhasına ilişkin genel prensiplerin ortaya konulması ve Yönetmelik'te belirtilen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yükümlülüklerin yerine getirilmesi için Türkiye İş Bankası A.Ş. (Banka) genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

3. KAPSAM

Politika; Kanun kapsamındaki tüm gerçek kişi gruplarının otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla Banka tarafından işlenen tüm kişisel verilerini kapsar.

Kanun çerçevesinde temel olarak, “verileri işlenen gerçek kişiler” koruma altına alınmakla birlikte, “bir gerçek kişinin belirlenmesini sağlayan” tüzel kişiye ait veriler de Kanun'un, dolayısıyla Politika'nın kapsamında yer almaktadır.

Politika, elektronik ve elektronik olmayan kayıt ortamlarını düzenlemektedir. Bankamız iş süreçlerinde kullanılan, uygulamalara girilen, bu uygulamalarla üretilen ve sistemler arası veya dış sistemlerle yapılan bilgi alışverişlerinde kullanılan ve veri depolama alanında saklanan yapısal ve yapısal olmayan veriler ile fiziki belgeler Politika çerçevesinde değerlendirilir.

4. TANIMLAR

Banka: Türkiye İş Bankası A.Ş.,

Kanun: Kişisel Verilerin Korunması Kanunu,

BDDK: Bankacılık Düzenleme ve Denetleme Kurumu,

İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kayıt Ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi,

Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,

Özel Nitelikli Kişisel Veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler,

Periyodik İmha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi,

Politika: Türkiye İş Bankası A.Ş. Kişisel Verilerin Korunması Politikası'nın ayrılmaz bir parçası olan Kişisel Veri Saklama ve İmha Politikası,

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi,

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi (bu Politika çerçevesinde Türkiye İş Bankası A.Ş.),

İlgili Kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri ifade etmektedir.

5. TEMEL ESASLAR

5.1. Kişisel Veri Envanteri Oluşturulması ve Yönetimi

Banka, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür. Bu yükümlülük; iş süreçlerine bağlı olarak gerçekleştirilen veri işleme faaliyetlerinin işleme amacı, veri kategorisi, veri aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirildiği, kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yurt dışına aktarımı öngörülen kişisel verileri ve hukuka aykırı işlemenin önlenmesi için veri güvenliğine ilişkin olarak alınan tedbirleri içeren envanter düzenlenerek yerine getirilir.

Envanter, faaliyet bazında ve yukarıda belirtilen detayda sağlıklı şekilde oluşturulur ve gerektiğinde güncellenir.

Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde envanterde belirtilen saklama ve imha süreleri dikkate alınır.

5.2. Kişisel Verilerin Saklanması ve İmhasını Gerektiren Sebepler

Banka, nezdindeki kişisel verileri Kişisel Verilerin Korunması Politikasına uygun olarak, Kanun ile düzenlenen temel prensipler ve şartlar çerçevesinde işler; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, bu verilere hukuka aykırı erişimleri önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alır.

Kişisel verilerin işlenmesine yönelik iş ihtiyaçlarının, amaç unsurunun ve Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, işleme şartları ortadan kalkan kişisel veriler, ilgili veri sahibi iş birimi kararıyla, Yönetmeliğin 7. maddesinde belirtilen ilkeler çerçevesinde, 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir. Konuya ilişkin Kişisel Verileri Koruma Kurulunca alınmış bir Karar ve/veya kesinleşmiş bir mahkeme kararının mevcudiyeti halinde gerekli hukuki değerlendirmenin yapılmasının ardından uygun aksiyon alınır.

Banka, işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç altı aylık periyodlar içerisinde, kullandıkları tüm veri kayıt ortamlarında gözden geçirir. Kişisel verileri işlenen gerçek kişilerin başvurusu ya da Kurulun veya bir mahkemenin bildirimi üzerine, periyodik denetleme süresine bakmaksızın veri kayıt ortamlarında bu gözden geçirme gerçekleştirilir.

Periyodik ya da herhangi bir anda yapılan gözden geçirmeler neticesinde veri işleme şartlarının tamamının ortadan kalkmış olduğu tespit edildiğinde, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verilir.

Kişisel verilerin periyodik imha süresi, Bankanın veri ve belge yönetimi uygulamalarına uygun şekilde belirlenir; ancak bu süre altı ayı geçemez.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

Kişisel verilerin muhafazasında ve imhasında, teknolojik imkânlar ve maliyetler değerlendirilerek, veri bütünlüğü ve iş sürekliliğinin zedelenmemesi gereği gözetilerek, uygun tüm teknik ve idari tedbirler alınır. Veri ve belge yönetiminde Bankanın ilgili dâhili mevzuat düzenlemeleri doğrultusunda aksiyon alınır.

Bir ilgili kişinin Kanunun 13. maddesine istinaden Banka'ya başvurarak kendisine ait kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini talep etmesi halinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri imha eder ya da bir sonraki periyodik imha işlemi kapsamına alınmasını sağlar. Banka, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, bu durum derhal aktarım yapılan üçüncü kişiye bildirilir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, ilgili kişilerin verilerinin silinmesi veya yok edilmesine yönelik talepleri Banka tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı ilgili kişiye en geç 30 gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin ya da Bankanın dijital kanallarında kimlik doğrulamasının yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara yönlendirilecektir.

6. GÖZETİM/DENETİM

İş süreçlerinin Politika esasları çerçevesinde tasarlanması ve buna uygun şekilde işletilmesinin sağlanması, Banka'nın sorumluluğundadır. Banka, bu politika hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır.

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

1. AMAÇ VE KAPSAM

Bu politikanın amacı; ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikte olmaları nedeniyle, Banka tarafından ve Banka adına işlenen özel nitelikli kişisel verilerin

korunmasına yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir süreç ve yöntemleri belirlemektir.

İşbu Özel Nitelikli Kişisel Verilerin Korunması Politikası, 6698 sayılı Kişisel Verilerin Korunması Kanunu başta olmak üzere ilgili mevzuat hükümleri uyarınca Özel Nitelikli Kişisel Verileri korumaya yönelik yükümlülüklerini yerine getirirken ve Özel Nitelikli Kişisel verileri işlerken Banka içinde uyulması gereken esasları belirlemektedir.

Bu politika, Banka tarafından ve Banka adına işlenen Özel Nitelikli Kişisel Verilere yönelik tüm faaliyetleri kapsar ve söz konusu faaliyetlere uygulanır.

Bu politika, Türkiye İş Bankası A.Ş. Kişisel Verilerin Korunması Politikası'nın ayrılmaz bir parçasıdır.

2. TANIMLAR

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza,

Banka: Türkiye İş Bankası A.Ş.,

Kanun: Kişisel Verilerin Korunması Kanunu,

İlgili Kişi: Kişisel verisi işlenen gerçek kişi,

Kanun: Kişisel Verilerin Korunması Kanunu,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi,

Özel Nitelikli Kişisel Veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler,

Özel Nitelikli Kişisel Verilerin İşlenmesi: Kanunda öngörülen hallerde ya da ilgilinin açık rızası alınarak, özel nitelikli 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,

Politika: Türkiye İş Bankası A.Ş. Kişisel Verilerin Korunması Politikası'nın ayrılmaz bir parçası olan Özel Nitelikli Kişisel Verilerin Korunması Politikası,

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi,

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi,

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi (bu politika çerçevesinde Türkiye İş Bankası A.Ş.) anlamına gelmektedir.

3. TEMEL ESASLAR

Politika gereklerine tüm Banka çalışanları ve özel nitelikli kişisel verinin paylaşıldığı taraflarca uyulması zorunludur. 3. tarafların politikaya uyumu, ilgili taraflarla yapılan hizmet sözleşmelerinde yer verilen hükümler ile sağlanır ve bu konuda gerekli tedbirler alınır.

Banka, işbu politikada belirtilen önlemlerin yanı sıra Kişisel Verilerin Korunması Kanunu'nun 12. Maddesinde belirtildiği şekilde gerekli tüm idari ve teknik tedbirleri faaliyet alanları gözetilerek alır.

3.1. Özel nitelikli kişisel veriler, kanunda belirtilen ilkeler ve şartların mevcudiyeti halinde usulüne uygun olarak işlenir.

3.2. Özel nitelikli kişisel veriler çok gizli kapsamında tutulur işlenir ve saklanır.

3.3. Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlarla ilgili aşağıdaki prosedürler uygulanır:

- Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilir.

- Gizlilik sözleşmeleri yapılır.

- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamı ve süreleri net olarak tanımlanır.

- Periyodik olarak yetki kontrolleri gerçekleştirilir.

- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılır. Bu kapsamda, Banka tarafından kendisine tahsis edilen envanter iade alınır.

3.4. Özel nitelikli kişisel verilerin elektronik ortamda işlenmesi, muhafaza edilmesi ve/veya erişilmesi durumunda aşağıdaki prosedürlere uyulur:

- Bu nitelikteki veriler Kriptografik yöntemler kullanılarak muhafaza edilir.

- Kriptografik anahtarlar güvenli ortamlarda tutulur.

- Veriler üzerinde gerçekleştirilen işlemlere dair yeterli iz kayıtları tutulur ve bu kayıtların güvenliği sağlanır.

- Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilir, gerekli güvenlik testleri düzenli olarak yapılır/yaptırılır, test sonuçları kayıt altına alınır.

- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmeleri yapılır ve bu yazılımların güvenlik testleri düzenli olarak yapılır/yaptırılır, test sonuçları kayıt altına alınır.

- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanır.

3.5. Özel nitelikli kişisel verilerin fiziksel ortamda işlenmesi, muhafaza edilmesi ve/veya erişilmesi durumunda aşağıdaki prosedürlere uyulur:

- Ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınır.

- Ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenir.

3.5. Özel nitelikli kişisel verilerin aktarılması durumunda aşağıdaki prosedürlere uyulur:

- Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılır.

- Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenir ve kriptografik anahtarlar farklı ortamda tutulur.

- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP/FTPS yöntemleriyle veri aktarımı gerçekleştirilir.

- Verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınır ve evraklar çok gizli derecesinde gönderilir.

4. GÖZETİM/DENETİM

İş süreçlerinin Politika esasları çerçevesinde tasarlanması ve buna uygun şekilde işletilmesinin sağlanması, Banka'nın sorumluluğundadır. Banka, bu politika hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır.