

# **KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI**

## **1. GİRİŞ**

Bu politikanın amacı; Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı'nda ("Vakıf") kişisel verilerin korunması ve işlenmesine ilişkin prensiplerin belirlenmesidir.

## **2. KAPSAM**

Bu politikanın kapsamı; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin Vakfımıza sunulan ya da Vakfımız tarafından elde edilen, özel nitelikli kişisel veriler de dahil olmak üzere, her türlü bilginin ("kişisel veri") işlenmesi ve korunması sürecidir.

Vakfımız işbu politkada tarif edilen yöntemler aracılığıyla, (i) vakıf üyeleri, vakıf üyeleri ile bağlantılı hak sahipleri ve daha önceden Vakıf üyesi olup mevcut durumda Vakıf'tan yararlanma hakkı sonlanan ve Vakıf üyesi olmayan kişilerin, kimlik bilgileri, iletişim bilgileri, görsel kayıtları, sağlık bilgileri, biyometrik verileri, finansal bilgileri, eğitim ve özgeçmiş bilgileri gibi kişisel veriler ve özel nitelikli kişisel veri niteliğindeki verilerini, (ii) Vakıf'ın faaliyetleri ve süreçlerini yöneten TSKB çalışanlarının kimlik bilgileri, iletişim bilgileri, görsel kayıtları kişisel verilerini, (iii) Vakıf'a gelen ziyaretçilerin kimlik bilgileri ve görsel kayıtları gibi kişisel verilerini, (iv) Vakıf ile hukuki ilişki içinde olan gerçek kişilerin kimlik bilgileri, iletişim bilgileri gibi kişisel verilerini ve (v) Vakıf nezdinde yapılan üyelik kontrol başvuruları neticesinde, başvuruya konu gerçek kişiler ve varsa bu kişilerin eş ve çocuklarının kimlik verileri gibi kişisel verilerini Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları kapsamında işlemekte olup bu doğrultuda işlenen tüm kişisel veriler bu politikanın kapsamındadır.

## **3. KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİNE İLİŞKİN UYGULAMALAR VE ALINAN TEDBİRLER**

Bu kapsamda Vakıf kişisel verilerin hukuka uygun olarak işlenmesini ve korunmasını sağlamak için, çalışanına konuya ilişkin eğitimler verdiği gibi, teknolojik imkânlar doğrultusunda teknik ve idari tedbirleri alır. Kişisel verileri işlenenler mevzuatın öngördüğü şekilde bilgilendirilir. Elde edilen kişisel verilerin gizli tutulmasına azami özen gösterilmektedir ve Vakfımız ile kişisel verilerini elektronik ortamda ya da sözlü/yazılı olarak paylaşanların kişisel verileri ancak ilgili kişinin rızası ya da mevzuatın izin verdiği durumlarda üçüncü kişiler ile paylaşılır. Kişisel verileri işlenenlerin Vakfımıza yönelttiği taleplerin etkin bir şekilde sonuca ulaştırılması içinse gerekli mekanizmalar

kurulur. Kişisel veri olarak çeşitli kanallardan Vakfa gelen yazılı, basılı ya da elektronik ortamdaki kişisel verilerin tespiti ve uygun kontrollerin tesis edilmesi, bu verilerin saklanmasına ilişkin gereken güvenli ortamların hazırlanması ve en önemlisi de bu verilere erişimin kısıtlı sayıda ve yetkili kişiler tarafından gerçekleştirilmesi için gerekli gayret gösterilir.

#### **4. KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİNE İLİŞKİN TEMEL İLKELER**

Kişisel Verilerin işlenmesinde gözetilen temel ilkeler aşağıdaki şekildedir:

- a) Kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak işlenir.
- b) Kişisel verilerin doğru olarak işlenmesine özen gösterilir ve gerektiğinde verilerde güncelleme yapılır.
- c) Kişisel verilerin hangi amaçlar için işleneceği belirli ve açıktır ve söz konusu amaçlar meşrudur. Kişisel verilerin hangi amaçlar için işlenebileceği konusunda ilgili kişi bilgilendirilir.
- ç) Kişisel veriler hangi amaç için işleniyorsa bu amaçla bağlantılı, sınırlı ve ölçülüdür.
- d) Kişisel veriler işlendikleri amaç için gerekli olan süre kadar muhafaza edilir. Bu kapsamda, ilgili mevzuatta öngörülmesi durumunda kişisel veriler bu süre boyunca saklanır. Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre düzenlenmemişse, ilgili veri yürütülen faaliyet ile bağlı olarak Vakfımız uygulamaları ve ticari yaşamının teamülleri uyarınca saklanması gerektiren süre kadar saklanır ve daha sonra niteliğine göre silinir, yok edilir veya anonim hale getirilir.

Kişisel verilerin işlenmesi konusunda aşağıdaki hallerde ilgili kişinin açık rızası olmaksızın kişisel veriler işlenebilir:

- a) Kanunlarda açıkça öngörülmesi.
- b) 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.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

## **5. KİŞİSEL VERİLERİN İŞLENME AMAÇLARI**

Vakfımızın mensuplarının kişisel verileri yukarıda belirtilen temel prensipler gözetilerek, Vakfımızın mensuplarının, bunların bakmakla yükümlü olduğu hak sahibi kişilerin, diğer hak sahiplerinin ve daha önceden Vakıf üyesi olup mevcut durumda Vakıf'tan yararlanma hakkı sonlanan ve Vakıf'ın üyesi olmayan kişilerin yukarıda bahsi geçen kişisel verileri ve özel nitelikli kişisel verileri, usulüne uygun olarak Vakfımız hizmetlerinden yararlanabilmesi ve kendileri ile iletişime geçilebilmesi, T.C. Anayasası, Sosyal Güvenlik mevzuatı, Vakıflar Kanunu vb. yasal mevzuat ile Vakıf Senedi ve Vakıf düzenlemeleri de dahil olmak ancak bunlarla sınırlı olmamak üzere, Vakfımızın tabi olduğu ilgili yasal mevzuat kapsamındaki yükümlülüklerin yerine getirilmesi, Vakfımızın taraf olduğu sözleşmelerin akdedilebilmesi ve gereğinin yerine getirilmesi, Vakfımızın hizmetlerinin sunulabilmesi ve Vakfımızın yükümlülüklerini yerine getirebilmesi için gerekli görülen veri tabanının oluşturulması, tüm kayıt ve belgelerin düzenlenmesi, Vakfımızdan talep edilen her türlü yardım ve hizmetlere ilişkin işlemlerin gereği gibi ve kesintisiz olarak gerçekleştirilmesi, Vakıf içi ve ilgili resmi kurumlarla iletişimin sağlanması, Resmi kurumlar ve mevzuat tarafından öngörülen bilgi saklama, raporlama, bilgilendirme ve diğer yükümlülüklerine uyulması ve gerektiğinde hukuki taleplere karşı savunma hakkının kullanılması amacı ile, anılan hukuki sebeplere dayanılarak veri sorumlusu sıfatı ile hareket eden Vakfımız tarafından işlenmektedir.

Yukarıdakilerin yanı sıra, (i) Vakıf faaliyetleri ve süreçlerini yöneten TSKB çalışanlarının, (ii) Vakıf'a gelen ziyaretçilerin ve (iii) Vakıf ile hukuki ilişki içinde olan gerçek kişilerin yukarıda bahsi geçen kişisel verileri iş ve iletişim faaliyetlerinin yürütülmesi, sözleşme süreçlerinin yürütülmesi, erişim yetkilerinin yürütülmesi, organizasyon ve etkinlik yönetimi, fiziksel mekan ve bilgi güvenliğini sağlanması amacıyla, veri sorumlusu sıfatı ile Vakfımız tarafından işlenmektedir. Son olarak, Vakıf ile aynı hukuki mahiyetteki diğer vakıflar ya da bizzat ilgili kişiler tarafından Vakıf nezdinde yapılan üyelik kontrol başvuruları neticesinde, başvuruya konu gerçek kişiler ve varsa bu kişilerin eş ve çocuklarının kimlik verileri, Vakıf bünyesinde üyeliklerinin mevcut olup olmadığının tespiti amacıyla, Vakıf tarafından işlenmektedir.

## **6. KİŞİSEL VERİLERİN PAYLAŞILABİLECEĞİ KİŞİ VE KURUMLAR**

Kişisel Veriler Vakfımızın ilgili çalışanlarına, işyeri hekimine, hastanelere, ambulans hizmeti sunan kurumlara ve diğer sağlık kurum ve kuruluşlarına, aktüerlere, ilgili mevzuat hükümlerinin izin verdiği ve/veya zorunlu kıldığı kişi veya kuruluşlara, mahkemeler, icra daireleri ve diğer resmi kurum ve kuruluşlara, faaliyetlerimizi yürütmek üzere hizmet aldığımız, işbirliği ya da anlaşma yaptığımız denetim şirketleri, yazılım şirketleri, sigorta şirketleri gibi gerçek ve tüzel kişilere ve/veya kurum ve kuruluşlara yukarıda belirtilen amaçlarla aktarılabilir.

Yukarıda bahsi geçen ilgili kişilerin kişisel verileri ve/veya özel nitelikli kişisel verileri, Vakıf'ın hizmet aldığı aktüerlere yukarıda belirtilen amaçlar dahilinde aktarıldıktan sonra, veri işleyen sıfatıyla hareket eden aktüerler tarafından aktüerya hizmetlerinin yürütülebilmesi ve yönetimi amacıyla söz konusu aktüerlerle bağlantılı, merkezi yurt dışında bulunan diğer aktüerlere aktarılabilir.

Vakıf üyelik sürecinin değerlendirilmesi ve yönetimi kapsamında Vakıf üyesi olan/olacak gerçek kişilerin ve varsa bu kişilerin eş ve çocuklarının kimlik verileri Vakıf ile aynı hukuki mahiyetteki diğer vakıflara, ilgili gerçek kişilerin ve varsa bu kişilerin eş ve çocuklarının bu vakıflarda üyeliklerinin mevcut olup olmadığını tespit etmek amacıyla aktarılabilir.

Son olarak yukarıda bahsi geçen gerçek kişilere ait Vakıf tarafından elde edilmiş ya da elde edilecek kişisel veriler ve özel nitelikli kişisel veriler, bu verilerin depolanması ve muhafaza edilmesi amaçlarıyla, veri işleyen sıfatıyla hareket eden Türkiye Sınai Kalkınma Bankası A.Ş.'na aktarılmaktadır.

## **7. KİŞİSEL VERİLERİ İŞLENEN KİŞİLERİN HAKLARI**

Kişisel verileri Vakfımızca işlenenler Vakfımıza başvurarak, kişisel verilerinin; a) işlenip işlenmediğini öğrenme, b) işlenmişse bilgi talep etme, c) bunlara erişim talep etme ve bu verileri isteme ç) işlenme amacını ve amacına uygun kullanılıp kullanılmadığını öğrenme, d) yurt içinde / yurt dışında aktarıldığı üçüncü kişileri bilme, e) eksik / yanlış işlenmişse düzeltilmesini isteme, f) Kişisel Verilerin Korunması Kanunu'nun 7. ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmelik'in 9.maddesinde öngörülen şartlar çerçevesinde ve sosyal güvenlik mevzuatı ile Vakfımız mevzuatı uyarınca hak sahipliğinin tespitine yönelik zorunlu olarak herhangi bir süreye tabi olmaksızın saklanması gereken kişisel veriler haricinde kalan kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini isteme, g) aktarıldığı üçüncü kişilere yukarıda sayılan (e) ve (f) bentleri uyarınca yapılan işlemlerin bildirilmesini isteme, ğ) münhasıran otomatik sistemler ile analiz edilmesi nedeniyle aleyhlerine bir sonucun ortaya çıkmasına itiraz etme, h) kanuna aykırı olarak işlenmesi sebebiyle zarara uğramaları hâlinde zararın giderilmesini talep etme hakkına sahiptir.

Söz konusu hususlarda Vakfımızın mevzuattan doğan hakları saklıdır. Makul olmayacak düzeyde yinelenen, orantısız düzeyde teknik çaba gerektiren, başkalarının gizliliğini tehlikeye atan istekler haricinde, söz konusu hakların etkin bir şekilde sağlanabilmesi için azami gayret gösterilir.

# KİŞİSEL VERİ SAKLAMA İMHA POLİTİKASI

## 1. AMAÇ VE KAPSAM

Kişisel Veri Saklama İmha Politikası'nın amacı; Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı'nda ("Vakıf") işlenen kişisel verilerin, işlendikleri amaç için gerekli olan azami süreler ile silinme, yok edilme ya da anonim hale getirilme süreçlerinin belirlenmesi ve bu süreçlerde görev alacak kişilerin rol ve sorumluluklarının tanımlanmasıdır.

Vakıf tarafından işbu politkada tarif edilen yöntemler aracılığıyla, (i) vakıf üyeleri, vakıf üyeleri ile bağlantılı hak sahipleri ve daha önceden Vakıf üyesi olup mevcut durumda Vakıf'tan yararlanma hakkı sonlanan ve Vakıf üyesi olmayan kişilerin, kimlik bilgileri, iletişim bilgileri, görsel kayıtları, sağlık bilgileri, biyometrik verileri, finansal bilgileri, eğitim ve özgeçmiş bilgileri gibi kişisel veriler ve özel nitelikli kişisel veri niteliğindeki verileri, (ii) Vakıf'ın faaliyetleri ve süreçlerini yöneten TSKB çalışanlarının kimlik bilgileri, iletişim bilgileri, görsel kayıtları kişisel verileri, (iii) Vakıf'a gelen ziyaretçilerin kimlik bilgileri ve görsel kayıtları gibi kişisel verileri, (iv) Vakıf ile hukuki ilişki içinde olan gerçek kişilerin kimlik bilgileri, iletişim bilgileri gibi kişisel verileri ve (v) Vakıf nezdinde yapılan üyelik kontrol başvuruları neticesinde, başvuruya konu gerçek kişiler ve varsa bu kişilerin eş ve çocuklarının kimlik verileri gibi kişisel verileri Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları kapsamında işlemekte olup bu doğrultuda işlenen tüm kişisel veriler bu politikanın kapsamındadır

Bu Politika'nın kapsamını; kişisel verilerin azami saklama süreleri ile kişisel verilerin hukuka uygun olarak saklanması ve imha edilmesi için alınmış teknik ve idari tedbirler, Vakıf bünyesinde ilgili süreçlerin yürütülmesinde görev alanlar ile kayıt ortamları oluşturmaktadır;

## 2. DAYANAK

İşbu politika, 07.04.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 28.10.2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5. ve 6. maddeleri doğrultusunda oluşturulmuştur.

### 3. TANIMLAR

**Vakıf:** Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı

**Kanun:** 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,

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

**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 işlemi,

**Veri Sorumlusu:** Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı'nı,

**Kurul:** Kişisel Verileri Koruma Kurulu'nu,

**Anonim Hale Getirme:** Kişisel Verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

**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 İşleme Envanteri:** Kişisel Verileri işleme faaliyetlerinin; Kişisel Verilerin işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturulan ve Kişisel Verilerin işlendikleri amaçlar için gerekli olan azami süreyi, aktarımı öngörülen Kişisel Verilerin ve veri güvenliğine ilişkin alınan tedbirlerin açıklanarak detaylandırıldığı envanteri,

**Kişisel Veri Saklama ve İmha Politikası/Politika:** Veri sorumlularının, Kişisel Verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları iş bu politikayı,

**Periyodik İmha:** Kanun'da yer alan Kişisel Verilerin işleme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama ve İmha Politikası'nda belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi,

**Vakıf Senedi:** Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı senedini

**Veri Kayıt Sistemi:** Kişisel Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

**Kişisel Verilerin Korunması ve İşlenmesi İlkeleri:** Vakıf tarafından hazırlanan ve Kişisel Verilerin korunması ve işlenmesine ilişkin genel esasları belirten ilkeleri,

**Kişisel Veri Saklama ve İmha Prosedürü:** Kişisel Veri Saklama ve İmha Politikası'nda belirtilen şekilde işlem kurallarını detaylı olarak düzenlemek amacı ile hazırlanan prosedürü,

**İlgili Kullanıcı:** KVK görevlisi hariç olmak üzere Veri Sorumlusu organizasyonu içerisinde veya Veri Sorumlusu'ndan aldığı yetki ve talimat doğrultusunda Kişisel Verileri işleyen kişileri ifade eder.

**KVK görevlisi:** Kişisel verilerin saklama ve imha süreçlerine ilişkin olarak Vakıf tarafından Vakıf'ın faaliyetleri ve süreçlerini yöneten TSKB çalışanlarından görevlendirilen ve işbu politikanın 3. Başlığı altında unvanına, birimine ve görev tanımına yer verilen kişi ya da kişileri ifade eder.

#### **4. KAYIT ORTAMLARI**

İşbu politika kapsamında kişisel veriler, Vakıf tarafından ve Vakıf adına veri işleyen sıfatıyla hareket eden TSKB tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

- Elektronik Kayıt Ortamları: Vakfın ilgili prosedürlerinde açıklanan, Vakfın Veri Tabanı Sunucusu, Yedekleme Medyaları gibi Vakıf tarafından kullanılan her türlü sunucu
- Fiziki Kayıt Ortamları: Arşiv, dolaplar ve kasa dairesi olmak üzere kişisel verilerin fiziki olarak saklandığı ortamlar

#### **5. SORUMLULUK**

Vakıf, aşağıdaki görev ve sorumlulukları yerine getirir:

- Kişisel Verilerin saklama süresine uygunluğunu sağlamak,
- Periyodik imha döneminde kişisel veri imha sürecinin yönetimini gerçekleştirmek,
- Politika'yı asgari olarak yıllık bazda gözden geçirmek,
- Politika'yı esas alarak işlem kurallarını detaylı düzenleyecek Kişisel Veri Saklama ve İmha Prosedürü ve gerekli gördüğü diğer prosedürleri düzenlemek ve yayımlamak,

- Politika ve prosedürlerin uygulanması için gerekli görev dağılımını yapmak, uygun gördüğü kişileri yetkilendirmek ve Kanun'a uyum konusundaki eğitimleri organize etmek,
- Kanununun 12. maddesi uyarınca alınan her türlü teknik ve idari tedbirlerin uygulanmasını takip etmek ve denetimini planlamak,
- Kanun ve ilgili mevzuata uyumun sağlanması için yapılması gereken hususları tespit etmek, uygulanmasını gözetmek ve gerekli koordinasyonu sağlamak,
- Kişisel Verileri işlenen gerçek kişiler tarafından yapılan başvuru ve taleplerle ilgili süreçlerin takibini yapmak ve Kanun ve/veya politika ve prosedürün uygulanması ile ilgili ortaya çıkabilecek sorunların çözümü için gerekli aksiyonların alınmasını sağlamak,
- Kurul ile olan ilişkileri yürütmek.

Kişisel verilerin saklama ve imha süreçlerine ilişkin olarak Vakıf tarafından Vakıf'ın faaliyetleri ve süreçlerini yöneten TSKB çalışanlarından bir KVK komitesi yetkilendirilecek olup söz konusu komitede görevli çalışanların unvanına, birimine ve görev tanımlarına aşağıda yer verilmektedir:

Unvan	Birim / Departman	Görev
Vakıf Müdürü Vakıf Yöneticisi (Üye ve Emeklilik İşlemlerinden Sorumlu Vakıf Yöneticisi – Sağlık İşlemlerinden Sorumlu)	Vakıf Departmanı	Politikanın yürütülmesinden ve çalışanların politikaya uygun hareket etmesinden sorumludur. Periyodik imha işlemlerini gerçekleştirmekten sorumludur.

## 6. VERİLERİN SAKLANMASINA VE HUKUKA AYRIKI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİNE İLİŞKİN GÜVENLİK ESASLARI

Vakıf tarafından Kişisel Verilerin Korunması ve İşlenmesi Politikası kapsamında temin edilen veriler, Kişisel Veri İşleme Envanteri'nde listelenen ve Kanunda belirtilen kurallar çerçevesinde sınıflandırılır.

Bu çerçevede Politika'ya temel teşkil eden sınıflandırma metodolojisi olarak Kanunda yer alan Kişisel Veri tanımlamaları kullanılmıştır. Bu kapsamda,

- Grup 1/Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veriyi,

- Grup 2/Özel nitelikli kişisel veri: Kişilerin ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep ve diğer inançları, kılık ve kıyafet, dernek, vakıf ya da sendika üyelikleri, sağlık, cinsel hayat, ceza mahkûmiyeti ve biyometrik ve genetik verileri,
- Grup 3/Diğer veri: Kişisel Veri tanımı kapsamına girmeyen verileri ifade etmektedir.

Vakıf tarafından üç ayrı sınıfta tasniflenen kişisel veriler ve özel nitelikli kişisel veriler veri işleyen sıfatı ile hareket eden TSKB bünyesinde saklanacak ve muhafaza edilecek olup bu saklanma ve muhafaza edilme sürecinde verilerin güvenliğini sağlamak adına bazı kural ve çerçeveler belirlenmiştir.

Bu bağlamda Kişisel Veri ve Özel Nitelikli Kişisel Veri olarak belirlenen 1. ve 2. Gruba ait olan verilerin güvenli bir şekilde saklanması için gereken teknik ve idari tedbirler alınmalıdır. Alınması gereken teknik ve idari tedbirler "Vakıf Kişisel Veri Envanteri" üzerinde belirtilmiştir. Söz konusu teknik ve idari tedbirler aşağıda sıralanmaktadır:

- 1. ve 2. Gruba ait işlenen ve saklanan veriler mümkün olduğunca azaltılmıştır.
- 1. ve 2. Gruba ait verilere erişim başta KVK görevlileri olmak üzere yalnızca kısıtlı sayıda ve yetkili personelin erişimindedir.
- 1. ve 2. Gruba ait verilere erişim için KVK görevlilerinden izin alınmaktadır.
- 2. Gruba ait veriler kaydedildikleri veri tabanlarında şifreli/maskeli olarak saklanmaktadır.
- 2. Gruba ait veriler taşınabilir depo ortamlarına kaydedilmemektedir. İstisnai durumlarda, Sistem Destek Uzmanı tarafından tahsis edilecek şifreli depo ortamları kullanılmaktadır.
- 1. ve 2. Grupta yer alan veriler kişisel bilgisayarlar üzerindeki veri diskleri ve e-posta hesapları yerine TSKB tarafından özel tahsis edilmiş ortak veri depolama alanlarında saklanmaktadır.
- Vakfa özel olarak tahsis edilmiş ortak depolama alanlarının yetkileri yalnızca kısıtlı sayıda ve yetkili personelde bulunmakta, yetkiler yıllık olarak KVK görevlileri tarafından gözden geçirilmektedir.
- Yazılı olarak temin edilmiş ve saklanan 1. ve 2. Gruba ait veriler, kasa dairesi, kilitli dolap ve çekmecelerde, yetkisiz erişime sebebiyet vermeyecek şekilde saklanmaktadır.
- Arşivlenerek saklanması gereken 1. ve 2. Gruba ait verilerin bulunduğu TSKB bünyesindeki kasa dairesi ve arşiv odalarının kapıları kilitli olup bu odalara yalnızca yetkili personel tarafından erişim sağlanmaktadır.
- Arşiv hizmeti alınarak saklanan 1. ve 2. Gruba ait verilerin, taşınması ve aktarımı sırasında gerekli gizlilik sağlanarak, verilerin hizmet alınan firma yetkilileri tarafından erişilmesini engelleyecek kontroller tesis edilmeli, arşive gönderilen verilere ilişkin teslim tutanakları tutulmaktadır.
- 1. ve 2. Grupta yer alan veriler güncel anti-virüs sistemleri ve güvenlik duvarları ile korunmaktadır.

- Vakıf tarafından (I) aydınlatma metni, (ii) özel nitelikli kişisel veri güvenliğine yönelik politika ve prosedürler ve (iii) kişisel verilerin korunması ve işlenmesi politikası, kişisel verilere erişim yönetimi prosedürü, başvuru ve şikayet prosedürü, kişisel veri aktarım ve paylaşım prosedürü, veri ihlali bildirim gibi politika ve prosedürler hazırlanmış olup tüm politika ve prosedürler uygulanmaktadır.
- 1. ve 2. Grupta yer alan verilere yönelik olarak TSKB, TSKB çalışanları ve dış ilişkide bulunan tüm üçüncü kişilerle gizlilik sözleşmeleri imzalanmaktadır.
- 1. ve 2. Grupta yer alan veriler yedeklenmekte ve yedeklenen verilerin güvenliği de sağlanmaktadır.
- 2. Grupta yer alan verileri yönelik olarak “Özel Nitelikli Kişisel Verilere İlişkin Politika” hazırlanmış olup bu politikada 2. Grupta yer alan verilerin güvenliğine ilişkin uygulanmakta olan özel bazı idari ve teknik tedbirlere yer verilmiştir.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır
- Vakıf içi periyodik denetimler yapılmakta ve yaptırılmaktadır.
- Vakıf bünyesinde kişisel verilerin işlenmesi ve saklanmasına yönelik olarak üçüncü kişiler tarafından Kanun kapsamında yapılan başvurular ve ilgili süreçler yıllık bazda raporlanmakta ve saklanmaktadır.
- 1. ve 2. Gruba ait verilerin hukuka aykırı olarak erişilmesinden ve uygun muhafaza edilmesinden Veri Sorumlusu sorumludur.
- 3. grupta yer alan veriler için Kanun kapsamında alınması gereken güvenlik önlemi bulunmamaktadır.

## **7. VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER**

Kişisel Veriler,

- Vakfımızın mensuplarının, bunların bakmakla yükümlü olduğu kişilerin, diğer hak sahiplerinin usulüne uygun olarak Vakfımız hizmetlerinden yararlanabilmesi ve kendileri ile iletişime geçilebilmesi,
- T.C. Anayasası, Sosyal Güvenlik mevzuatı, Vakıflar Kanunu vb. yasal mevzuat ile Vakıf Senedi ve Vakıf düzenlemeleri de dahil olmak ancak bunlarla sınırlı olmamak üzere, Vakfımızın tabi olduğu ilgili yasal mevzuat kapsamındaki yükümlülüklerin yerine getirilmesi,
- Vakfımızın taraf olduğu sözleşmelerin akdedilebilmesi ve gereğinin yerine getirilmesi,

- Vakfımızın hizmetlerinin sunulabilmesi ve Vakfımızın yükümlülüklerini yerine getirebilmesi için gerekli görülen veri tabanının oluşturulması, tüm kayıt ve belgelerin düzenlenmesi,
- Vakfımızdan talep edilen her türlü yardım ve hizmetlere ilişkin işlemlerin gereği gibi ve kesintisiz olarak gerçekleştirilmesi,
- Vakıf içi ve ilgili resmi kurumlarla iletişimin sağlanması,
- Vakıf ile ilgili iş ve iletişim faaliyetlerinin yürütülmesi, organizasyon ve etkinlik yönetimi,
- Vakıf'ın fiziksel mekan ve bilgi güvenliğini sağlanması,
- Vakıf ile ilgili ileride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünün yerine getirilmesi,
- Resmi kurumlar ve mevzuat tarafından öngörülen bilgi saklama, raporlama, bilgilendirme ve diğer yükümlülüklerine uyulması amacıyla Kanun'un 5. ve 6. maddelerinde belirtilen şartlar doğrultusunda saklanır.
- Kişisel Veriler, İşlenme ve saklanma amacının sona ermesi,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verisi işlenen ilgili kişilerin açık rızasını geri alması,
- Kanununun 11. maddesi kapsamında kişisel verisi işlenen ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin başvuru yapması ve başvurunun Vakıf tarafından uygun görülmesi,
- kişisel verisi işlenen ilgili kişinin hakları çerçevesinde Kurul'a şikayette bulunması ve Kurul'un söz konusu kişisel verilerinin silinmesi ve yok edilmesine ilişkin şikayeti kabul etmesi ya da
- ilgili mevzuat ve/veya Vakfımızın belirlediği saklama sürelerinin sonuna gelmesi halinde ise Kişisel Veriler, işbu Politika'da belirtilen esaslar çerçevesinde imha edilir.

## **8. VERİLERİN İLGİLİ MEVZUAT KAPSAMINDAKİ SAKLAMA SÜRELERİ**

Vakıf bünyesinde saklanan tüm Kişisel Veriler için saklama süreleri belirlenir. Saklama süreleri belirlenirken öncelikle ilgili mevzuat, ilgili mevzuat ile öngörülen bir süre yoksa Kişisel Veri işleme amacı için gereken süreler ve teamüller göz önünde bulundurulur. İlgili sürelere Kişisel Veri Envanteri'nde ve Sicil kaydında yer verilir.

Kişisel Veri İşleme Envanteri'nde bahsi geçen Kişisel Veriler, zamanaşımı süresini kesen ya da durduran herhangi bir hukuki durum olmadığı takdirde, aşağıdaki tabloda yer alan yasal düzenlemeler gereği saklanır ve saklama süresini takip eden ilk periyodik imha tarihinde imha edilir.

Sosyal Güvenlik Mevzuatı ve ilgili teamül gereği	Süresiz
Sair İlgili Mevzuat Gereği	İlgili mevzuatta öngörülen süre kadar
Genel dava zamanaşımı süresini düzenleyen Borçlar Kanunu'nun 146. maddesi gereği	10 Yıl
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suçta konu olması veya bir suç ile ilişkili olması durumunda Türk Ceza Kanunu'nun 66. ve 68. maddeleri gereği	Dava zamanaşımı ve Ceza Zamanaşımı müddetince

Yukarıda belirtilen saklama sürelerinin yanı sıra, Vakıf tarafından işlenen (i) kamera kayıtları [\_1ay\_] süreyle ve (ii) ziyaretçi kayıtları [\_10 yıl\_] süreyle saklanır ve saklama süresini takip eden ilk periyodik imha tarihinde imha edilir.

## 9. VERİLERİN İMHASINA İLİŞKİN GÜVENLİK ESASLARI

Vakıf tarafından Kişisel Verilerin Korunması ve İşlenmesi Politikası kapsamında temin edilen ve Kişisel Veri Envanteri'nde belirtildiği şekilde saklanan Kişisel Veriler, işleme amacı sona ermiş ya da ilgili mevzuatta ve/veya Politika'da belirtilen saklama sürelerinin sonuna gelinmişse, Kişisel Verisi işlenen gerçek kişinin kendi talebi üzerine ya da re'sen, kayıt ortamlarına uygun şekilde; Kişisel Verinin niteliğine uygun olarak belirlenecek silme, yok etme ya da anonimleştirme

süreçlerine tabi tutularak detayları Kişisel Veri Saklama ve İmha Prosedüründe gösterilen şekilde imha edilir.

Vakıf tarafından kullanılan İmha yöntemleri aşağıdaki şekildedir.

### 9.1. VERİLERİN SİLİNMESİ

Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilme işlemidir.

- Kişisel verilerin bulunduğu elektronik ve fiziksel ortamlar üzerinde silme işlemi gerçekleştirilmek üzere imha edilmesi işlemidir.
- Silme işlemi, verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve geri döndürülemez olacak şekilde gerçekleştirilir.
- Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar tarafından erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Silme yöntemine ilişkin ortamlar bazında örnekler aşağıda yer almaktadır:

Ortam Adı	Metot
Hizmet Olarak Uygulama Türü Bulut Çözümleri	Silme Komutu verilerek
Fiziksel	Karartma Yöntemi ile
Merkezi Sunucuda yer alan Ofis Dosyaları	İşletim sistemi üzerinden silme komutu/ izin üzerinde yer alan kullanıcıların erişimlerinin kaldırılması
Taşınabilir Medya (USB/Disk vb.)	Şifreli olarak saklanmalı ve uygun yazılım kullanılarak
Veritabanı	İlgili satırın veritabanı komutu ile

### 9.2. VERİLERİN YOK EDİLMESİ

Kişisel Verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Yok etme yöntemine ilişkin ortamlar bazında örnekler aşağıda yer almaktadır:

Ortam Adı	Metot
Yerel Sistemler	De-Manyetize etmek, fiziksel olarak yok etmek ve üzerine yazma metotları
Çevresel Sistemler	<ul style="list-style-type: none"><li>• Ağ Cihazları: Yerel Sistemlerde kullanılan metotlar ile</li><li>• Flash Tabanlı Ortamlar: ATA ve SCSI arayüzüne sahip ise &lt;block erase&gt; komutu, eğer ilgili arayüz desteklenmiyor ise üreticinin önerdiği yok etme metodu veya yerel sistemlerde kullanılan metotları ile</li><li>• Manyetik Bant: De-Manyetize, Yakma, Eritme gibi fiziksel olarak yok etme</li><li>• Manyetik Disk Üniteleri: De-Manyetize, Yakma, Eritme gibi fiziksel olarak yok etme</li><li>• Mobil Telefonlar: Yerel Sistemlerde kullanılan metotlar ile</li><li>• Optik Diskler: Fiziksel yok etme yöntemleri ile</li><li>• Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Yerel Sistemlerde kullanılan metotlar ile</li><li>• Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Yerel Sistemlerde kullanılan metotlar ile</li></ul>
Kağıt ve Mikrofiş Ortamları	<ul style="list-style-type: none"><li>• Ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölerek</li><li>• Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre Yerel Sistemlerde kullanılan metotlar ile</li></ul>
Bulut Ortamı	<ul style="list-style-type: none"><li>• İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin Yerel Sistemlerde kullanılan metotlar ile,</li><li>• Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,</li></ul>

### 9.3. VERİLERİN ANONİMLEŞTİRİLMESİ

Kişisel Verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemidir. Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir (örneğin: TCKN, Adı-Soyadı vb. verilerin maskeleyme/yıldızlama, toplulaştırma/kümülatif data oluşturma, veri türetme ve veri karması metodlarının kullanılması). Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Kişisel Verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleyme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Anonim hale getirilmiş Kişisel Verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmesi esas alınır.

### 10. İMHA SÜRECİNİN İŞLETİLMESİ

Vakıf bünyesinde saklanan Kişisel Veriler, saklama süreleri sona erdiğinde ve/veya Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalktığında, verilerin gizliliğini korumak suretiyle İmha sürecine tabi tutulurlar.

- 1. ve 2. Gruba ait verilerin, işlenmesini gerektiren sebepler ortadan kalktığında İmha sürecini işletmek Vakfın sorumluluğundadır. Bu veriler için belirlenecek İmha yöntemi Vakıf tarafından belirlenir.
- 1. ve 2. Gruba ait verilerin imha süreci KVK görevlisi tarafından başlatılır.
- Kişisel Verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanır.

Kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğü kapsamında aşağıdaki süreler dikkate alınır.

- Veri Envanterinde belirtilen saklama süresi kapsamında yükümlülüğün ortaya çıktığı tarihi takip eden ilk Periyodik İmha işleminde Kişisel Veriler silinir, yok edilir veya anonim hale getirilir.
- Periyodik İmha sürecinin zaman aralığı azami 6 (altı) aydır.

Vakıf bünyesinde Kişisel Verisi bulunan kişiler, Vakıf web sitesi üzerinde yayınlanan “Kişisel Veriler İletişim Formu” aracılığı ile söz konusu verilerin imha edilmesi için talepte bulunma hakkına sahiptir. Bu hakkın kullanılması durumunda:

- Kişisel Verileri işleme şartlarının tamamı ortadan kalkmışsa; talebe konu Kişisel Veriler silinir, yok edilir veya anonim hale getirilir. İlgili kişilerin silme veya yok etme talepleri Veri Sorumluları tarafından en geç otuz gün içerisinde sonuçlandırılır ve Kişisel Verilerinin silinmesini talep eden kişiye işlem hakkında bilgi verilir.
- Kişisel Verilerin işleme şartlarının tamamı ortadan kalkmış ve silinmesi talep edilen veri daha önce üçüncü kişilere aktarılmış ise; silme işleminin üçüncü taraf nezdinde de ivedilikle ve maksimum otuz gün içerisinde yapılması için bilgilendirmeyi yapar ve gerekli işlemlerin yapıldığına ilişkin üçüncü kişilerden bilgilendirme talep eder.
- Kişisel Verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Bu doküman yıllık olarak KVK görevlisi tarafından gözden geçirilir. Ancak, mevcut süreç işleyişinde değişiklik olması durumunda minimum bir yıllık gözden geçirilme süresi beklenmeden, süreç içerisindeki değişiklikler doküman içerisine KVK görevlisi tarafından yansıtılır.

# ÖZEL NİTELİKLİ KİŞİSEL VERİLERE İLİŞKİN POLİTİKA

## 1. GİRİŞ

Bu politikanın amacı; Türkiye Sınai Kalkınma Bankası A.Ş. Mensupları Munzam Sosyal Güvenlik ve Yardımlaşma Vakfı'nda ("Vakıf") özel nitelikli kişisel verilerin korunması ve işlenmesine ilişkin prensiplerin belirlenmesidir.

## 2. KAPSAM

Bu politikanın kapsamı; Vakfımıza sunulan ya da Vakfımız tarafından elde edilen, 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 verilerin ("özel nitelikli kişisel veri") işlenmesi ve korunması sürecidir.

## 3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİNE İLİŞKİN UYGULAMALAR VE ALINAN TEDBİRLER

I) Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik olarak:

- Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konusunda 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 yetkilerinin derhal kaldırılmalıdır, Veri sorumlusu tarafından kendine tahsis edilen veri envanteri iade alınır.

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

- Verilerin kriptografik yöntemler (Gizli Anahtarlı Kriptografi, Açık Anahtarlı Kriptografi, Sayısal İmza, Şifreleme Algoritmaları, SSL (Secure Socket Layer)) kullanılarak muhafaza edilir,
- Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulur,
- Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanır,

- d) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması / yaptırılması ve test sonuçlarının kayıt altına alınması süreçleri işletilir,
- e) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/ yaptırılması ve test sonuçlarının kayıt altına alınması süreçleri işletilmeli,
  - f) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanır.
- III) Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise,
  - a) Özel nitelikli kişisel verilerin bulunduğu ortam niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlarına karşı) alındığından emin olunur,
  - b) Bu ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenir.

#### **4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER**

Özel nitelikli kişisel verilerin işlenmesinde gözetilen temel ilkeler aşağıdaki şekildedir:

Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmadan işlenmemesi esas olup, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

Özel nitelikli kişisel verilerin işlenmesinde, Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemler alınır.

#### **5. KİŞİSEL VERİLERİN AKTARILMASINA İLİŞKİN TEMEL İLKELER**

Özel nitelikli kişisel verilerin aktarılmasında gözetilen temel ilkeler aşağıdaki şekildedir:

- a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle aktarılır,
- b) Taşınabilir bellek, CD, DVD, gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulur,
- c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yönetimiyle veri aktarımı gerçekleştirilir,

d) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” (Üzerinde çok gizli, gizli, özel ve hizmete özel ibaresi taşıyan evrak) formatında gönderilir.

**TÜRKİYE SINAİ KALKINMA BANKASI A.Ş.**  
**MENSUPLARI MUNZAM SOSYAL GÜVENLİK VE DAYANIŞMA VAKFI**  
**BİLGİ GÜVENLİĞİ POLİTİKASI**

**A. AMAÇ**

Bilgi Güvenliği Politikası (Politika) ile Vakıf bilgi varlıklarının güvenliğinin sağlanması, bilgi varlıklarına yönelik kasıtlı veya kasıtsız her türlü tehdidin belirlenmesi ve bu tehditlerin oluşturabileceği risklerin yönetilebilmesi amaçlanmaktadır.

**B. KAPSAM**

Bilgi Güvenliği Politikası, Vakfın ortam ve formata bakılmaksızın saklanan, iletişim halindeki ve işlenen fiziksel ve elektronik tüm bilgi ve verilerini kapsar. Politika, Vakıfta Banka tarafından görevlendirilen tüm çalışanlarına, yüklenicilere, tedarikçilere ve Vakıfla çalışan üçüncü kişilere uygulanır.

**C. İLKE VE ESASLAR**

- 1- Vakıf kanunlara, tüm yasal düzenlemelere, sektörel kurallara, anlaşmalardan doğan yükümlülüklerle ve iş ihtiyaçlarına uygun şekilde bilgi güvenliğini sağlamak üzere TSKB Bilgi Güvenliği Politikasına uygun şekilde operasyonunu gerçekleştirir.
- 2- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur. Bilgi varlıkları sahipleri atanır, sınıflandırılır ve sınıflandırmalarına uygun güvenlik ihtiyaçları ve kullanım kuralları belirlenir. Belirlenen seviyeler ve koruma tedbirleri Banka'nın ilgili prosedürlerinde detaylandırılır.
- 3- Sistemler, erişilen uygulama ve cihazlar sadece bankanın işlerinin yürütülmesi için kullanılır, iş dışı amaçlarla kullanılmaz. Tüm kaynaklar Bankanın yetkili çalışanları tarafından güvenlik veya bakım amaçlı düzenli ve düzenli olmayan aralıklarla izlenir.
- 4- Kişisel verilerin güvenliği için ilgili yasal düzenlemeler, yönetmelik veya mevzuata uyum sağlayacak önlemler alınır.
- 5- Vakıf bilgilerinin, sadece iş ihtiyaçları doğrultusunda yetkilendirilmesi, sadece yetki verilen amaçlarla kullanılması sağlanır. Vakıf genelinde rol ve sorumluluklar görevler ayrılığı ilkesine öre belirlenir ve bu doğrultuda kimlik doğrulama ve erişim yönetim sistemi tesis edilir.
- 6- İlgili mevzuatlara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli kontrol süreçleri tasarlanır.
- 7- Dış hizmet alımlarının yönetimi kapsamında Bilgi Güvenliği politika ve standartlarına uyum gözönünde bulundurulur.
- 8- Yaşanacak herhangi bir olumsuzluk karşısında faaliyetlerin ve üyelere olan sorumlulukların kesintiye uğramaması adına TSKB İş Sürekliliği politikalarında belirlenen ilke ve esaslara uyum gözetilir.
- 9- Bilgi güvenliği politikasına uymayan durumlar, TSKB Bilgi Güvenliği ve Kalite çalışanlarına bildirilir.

10- Bilgilerin deęeri, gizlilik seviyesi, kaybolma ve alınma tehlikesi ve tekrar elde etme kolaylığıyla uyumlu olarak fiziki ve mantıksal erişim güvenliği mekanizmaları kullanılarak bilgiler korunur. Bilginin Vakıf dıőına ıkarılması durumunda, bilginin iinde olduęu sınıflandırmaya gre aynı gizlilik ve koruma kuralları geerlidir.

#### **D. SORUMLULUKLAR**

Tm Vakıf alıőanları ve 3. Taraflar bu politikayı bilmek ve alıőmalarını bu kurallara uygun Őekilde yrtmekle ykmldr. Politikaya aykırı faaliyetler ile Vakıf bilgilerinin gizlilięini, btnlęn veya elveriŐlilięini tehlikeye dŐrecek davranıŐlar, İŐ Kanunu ve TSKB İnsan Kaynakları Ynetmelięi hkmlerince iŐ akdini feshe kadar varabilen disiplin iŐlemlerine neden olabilir.

#### **E. YRRLęE GİRİŐ VE GNCELLEME**

Politika, Vakıf Ynetim Kurulu tarafından onaylandıęı tarihte yrrlęe girer. Politika yılda en az bir kez ya da sistem yapısını veya risk deęerlendirmesini etkileyecek herhangi bir deęiŐiklik olması durumunda gzden geirilir ve gerekli grlmesi halinde gncellenir.