KREDİ GARANTİ FONU

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

1.1. Amaç

Kişisel verilerin T.C. Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve diğer ilgili mevzuata uygun olarak işlenmesi ve korunması, Kredi Garanti Fonu A.Ş. (KGF)' nin öncelikleri arasındadır.

İşbu Kişisel Verileri Saklama ve İmha Politikası (bundan sonra "Politika" olarak anılacaktır.), KGF tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek, kişisel verileri KGF tarafından işlenen kişileri bilgilendirilerek şeffaflığı sağlamak amacıyla hazırlanmıştır.

KGF tarafından kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, işbu Politikaya uygun olarak gerçekleştirilir.

Politika, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5. Maddesi çerçevesinde Envanter'e ve Kurum'un kararlarına uygun olarak hazırlanmıştır.

1.2. Kapsam

Politika; otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla KGF tarafından verileri işlenen Yararlanıcıların, Potansiyel Yararlanıcıların, Teminat Sağlayanların, Çalışanların, Çalışan Adaylarının, Ziyaretçilerin, Tedarikçilerin ve diğer üçüncü kişilerin kişisel verilerine ilişkindir. Bu Politika kapsamında olup Şirketimizin sahip olduğu ya da Şirketimizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. Kısaltmalar ve Tanımlar

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

Alıcı Grubu: KGF tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

Anonim Hâle Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

Anonimleştirme Yönetmeliği: KVKK 7/3 ve 22/1-(e) maddeleri uyarınca hazırlanan 16/11/2017 tarihli ve 30242 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hala Getirilmesi Hakkında Yönetmelik'i,

Çalışan/Çalışanlar: KGF'nin çalışanlarını,

Çalışan Adayı/Çalışan Adayları: KGF'ye iş ilişkisine girme amacıyla başvuran, özgeçmiş gönderen, görüşmeye giren tüm gerçek kişileri,
(Çalışan Adayı, işe alınması halinde çalışan grubu için verilen bilgiler kapsamında değerlendirilmelidir.)

Departman: KGF bünyesinde çalışanların görev ve sorumlulukları çerçevesinde oluşturulmuş olan her bir iş birimini,

Envanter: Kişisel Veri İşleme Envanterini,

İK Portal: Kredi Garanti Fonu A.Ş.'nin İnsan Kaynakları Bilgi İşletim Sistemi'ni,

İkincil Mevzuat: Kişisel Verileri Koruma Kurulu tarafından çıkarılan Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmeliği, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i, Veri Sorumluları Sicili Hakkında Yönetmeliği, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliği ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği ve ileride çıkarılabilecek tebliğ, yayımlanan ve yayımlanacak idari veya yargısal karar ve ilkeleri,

İlgili Kişi/Veri Sahibi: Kişisel verisi işlenen gerçek kişiyi,

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,

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

Kanun (KVKK): 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nu,

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,

KGF: Kredi Garanti Fonu A.Ş.'yi,

Kişi Grubu: KGF'nin kişisel verilerini işledikleri ilgili kişi kategorisini,

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 ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

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,

KOBİT: Kredi Garanti Fonu A.Ş.'nin Bilgi İşletim Sistemi'ni,

Kurul: Kişisel Verileri Koruma Kurulu'nu,

Kurum: Kişisel Verileri Koruma Kurumu'nu,

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 verileri,

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

Politika: İşbu Kişisel Veri Saklama ve İmha Politikası'nı,

Potansiyel Yararlanıcı: KGF'nin kredi garanti sisteminden yararlanma amacıyla KGF'ye başvuran gerçek kişileri ve/veya tüzel kişilerin gerçek kişi ortakları ve temsilcilerini,

Sicil: Kurum Başkanlığı tarafından tutulan veri sorumluları sicilini,

Sicil Yönetmeliği: 30 Aralık 2017 tarihli ve 30286 sayılı Resmi Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik'i,

Tedarikçi/Tedarikçiler: KGF'nin çalışanı sıfatına sahip olmayan ancak KGF'ye hizmet veren tüm tüzel kişilerin gerçek kişi temsilci ve personelini ve gerçek kişiler ile bunların gerçek kişi personellerini,

Üçüncü Kişiler: Diğer kişi gruplarına girmeyen KGF ziyaretçileri, muhtemel gayrimenkul alıcıları, yedieminler, yerel yönetim ve diğer kurum ve kuruluşların yetkilileri ve çalışanları başta olmak üzere tüm gerçek kişileri,

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişileri,

Veri Kategorisi: Kişisel verilerin ortak özelliklerine göre gruplandırıldığı veri konusu kişi grubu veya gruplarına ait kişisel veri sınıfını,

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

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kurum tarafından oluşturulan ve yönetilen bilişim sistemini,

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişileri,

Yararlanıcı: KGF'nin kredi garanti sisteminden yararlanan şahıs şirketi sahibi gerçek kişileri ve/veya tüzel kişilerin gerçek kişi ortakları ve temsilcilerini,

Yönetmelikler: Kurul tarafından çıkarılan Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik, Anonimleştirme Yönetmeliği, Sicil Yönetmeliğinin tamamını ifade eder.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

KGF'nin tüm departmanları ve çalışanları, sorumlu departmanda Politika kapsamında alınmakta olan tedbirlerin gereği gibi uygulanması, departman çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi ile

kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik tedbirler konularında sorumlu birimlere aktif olarak destek verir.
Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda belirtilmiştir.

Saklama ve İmha Süreçleri Görev Dağılımı:

UNVAN	**BİRİM**	**GÖREV**
Kurumsal İletişim ve Destek Hizmetleri Genel Müdür Yardımcısı	Kurumsal İletişim ve Destek Hizmetleri Genel Müdür Yardımcılığı	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi
Araştırma, Geliştirme ve Bilgi Teknolojileri Bölüm Müdürü	Araştırma, Geliştirme ve Bilgi Teknolojileri Bölüm Müdürlüğü	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulması
İç Denetim Bölüm Müdürü, İnsan Kaynakları ve Performans Yönetimi Bölüm Müdürü, Kurumsal İletişim ve Ürün Yönetimi Bölüm Müdürü, Muhasebe ve İdari İşler Bölüm Müdürü, Kredi Tahsis Genel Müdür Yardımcısı, KOBİS Bölüm Müdürü, Kredi Operasyon Bölüm Müdürü, PGS Bölüm Müdürü, Kredi Tahsis Bölüm Müdürü, Risk Yönetimi Genel Müdür Yardımcısı, Hukuk İşleri Bölüm Müdürü/Hukuk Müşaviri, Risk İzleme ve Tazmin Bölüm Müdürü, Takip Tasfiye (Hazine) Bölüm Müdürü, Takip Tasfiye (Özkaynak) Bölüm Müdürü.	Diğer Birimler	Görevlerine uygun olarak Politika'nın yürütülmesi

3. KAYIT ORTAMLARI

Kişisel veriler, KGF tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Kişisel Veri Saklama Ortamları:

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, Felaket Kurtarma Merkezi) Yazılımlar (KOBİT, İK-Portal) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) Kişisel bilgisayarlar (Masaüstü, dizüstü) Mobil cihazlar (telefon, tablet vb.) Optik diskler (CD, DVD vb.) Çıkartılabilir bellekler (USB, Hafıza Kart vb. Yazıcı, tarayıcı, fotokopi makinesi.	Kağıt Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) Yazılı, basılı, görsel ortamlar.

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

KGF tarafından; Yararlanıcıların, Potansiyel Yararlanıcıların, Teminat Sağlayanların, Çalışanların, Çalışan Adaylarının, Ziyaretçilerin, Tedarikçilerin ve diğer üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1. Saklamaya İlişkin Açıklamalar

Şirketimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süreler kadar saklanır.

4.1.1. Saklamayı Gerektiren Hukuki Sebepler

Şirketimizce kişisel veriler, Şirketimiz ve Şirketimizin faaliyetlerinin tabi olduğu mevzuattan doğan yükümlülüklerimizin yerine getirilmesi için Kişisel Verilerin Korunması Kanunu, Türk Ticaret Kanunu, Bankacılık Kanunu, Türk Borçlar Kanunu, Türk Medeni Kanunu, İcra İflas Kanunu, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, İş Sağlığı ve Güvenliği Kanunu, İş Kanunu, Gelir Vergisi Kanunu, Vergi Usul Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile yürürlükte olan diğer ikincil düzenlemeler ve Şirketimizin faaliyetlerinin tabi olduğu diğer tüm ilgili yasal mevzuat çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2. Saklamayı Gerektiren İşleme Amaçları

Şirketimiz faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek,
- Kurumsal iletişimi sağlamak,
- Şirket güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- KGF ile iş ilişkisinde bulunan gerçek/tüzel kişilerle irtibat sağlamak,
- Yasal raporlamalar yapmak,
- Çağrı merkezi süreçlerini yönetmek,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği, ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun, Şirketimiz tarafından kabul edilmesi veya ilgili kişi tarafından başvuru sonucu Kurulca başvurunun kabul edilmesi,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Şirketimiz tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği, özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde, KGF tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

KGF tarafından işlenen kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Sızma (Penetrasyon) testleri ile Şirketimizin bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- KGF'nin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- KGF içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- KGF, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için KGF tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- KGF internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamlarda yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2. İdari Tedbirler

Şirketimiz tarafından, işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Kişisel verilerin hukuka uygun işlenmesi, saklanması, imhası ile hukuka aykırı erişiminin önlenmesi konularında hukuksal uyum gerekliliklerinin sağlanması için ilgili iş birimleri özelinde farkındalık yaratılmakta; bu hususların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler, politikalar, bilgilendirme ve eğitimler yoluyla hayata geçirilmektedir.
- İş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak kişisel verilere erişim ve yetkilendirme süreçlerinde yetki matriksi uygulanmaktadır.
- Şirketimizce yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü bulunmaktadır.
- Kişisel veri işlemeye başlamadan önce Şirketimiz tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.

- Şirketimizce Kişisel veri işleme envanteri hazırlanmıştır.
- Şirketimiz, Kanun'un 12. maddesine uygun olarak, kendi bünyesinde gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları, Şirketin iç işleyişi kapsamında konu ile ilgili bölüme raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Kurum tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler, aşağıda gösterilen yöntemlerle silinir.

Kişisel Verilerin Silinmesi Yöntemleri:

VERI KAYIT ORTAMI	**AÇIKLAMA**
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim

	yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, KGF tarafından aşağıda gösterilen yöntemlerle yok edilir.

Kişisel Verilerin Yok Edilmesi:

VERİ KAYIT ORTAMI	AÇIKLAMA
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Şirketimizce kişisel veriler ilgili yasal mevzuat kapsamında ve iş bu politikada belirtilen gerekçeler ile amaçlar doğrultusunda işlenerek; saklama süresinin ilgili mevzuatlarda öngörülmesi durumunda bu mevzuatlarda belirtilen süre boyunca, ilgili mevzuatta bir süre düzenlenmemişse, uygulamalar ile ticari

yaşamının teamülleri uyarınca kişisel verinin işlenmesini gerektiren süre kadar saklanmakta, daha sonra silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Şirketimizce 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.

Şirketimiz tarafından faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak detaylı saklama ve imha süreleri Envanter'de düzenlenmekle birlikte süreç bazında saklama süreleri ise, işbu Politika kapsamında aşağıda yer almaktadır.

Süreç Bazında Saklama ve İmha Süreleri :

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
Şirket İşlemleri	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yararlanıcı Talepleri	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kurumsal İletişim	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İdari İşler	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bilgi Teknolojileri Süreçleri	İlgili faaliyet ve işlem müddeti + (*)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

(*) Aksine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça kişisel veriler, ilgili faaliyet ve işlem müddetinden sonra aşağıdaki tabloda belirtilen süreler boyunca saklanır.

Genel dava zamanaşımı süresini düzenleyen Borçlar Kanunu'nun 146. Maddesi gereği	10 yıl
Sair ilgili mevzuat gereği	İlgili mevzuatta öngörülen süre kadar
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması veya bir suç ile ilişkili olması durumunda Türk Ceza Kanunu'nun 66. ve 68. maddeleri gereği	Dava zamanaşımı ve Ceza Zamanaşımı

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince, periyodik imha süresi 6 ay olarak belirlemiştir. Buna göre, her yıl Mart ve Eylül aylarında periyodik imha işlemi gerçekleştirilir.

9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Kurumsal İletişim ve Ürün Yönetimi Bölüm Müdürlüğü'nde dosyasında saklanır.

10. POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.