

# LUDENS İLERİ FİNANSAL HİZMETLER VE DANIŞMANLIK LTD. ŞTİ

## KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

İşbu Kişisel Veri Güvenliğini Sağlama, Saklama ve İmha Politikası (“**Politika**”), 6698 Sayılı Kişisel Verilerin Korunması Kanunu (“**KVKK**” ya da “**Kanun**”) ve Kanun’un ikincil düzenlemesini teşkil eden Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“**Yönetmelik**”), ve Kişisel Verileri Koruma Kurumu (“**Kurum**”) sitesinde yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (“**Rehber**”) ile açıklanan tedbirler uyarınca belirlenen yükümlülükleri yerine getirmek ve verisi işlenen ilgili kişilerin kişisel verilerinin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile bu verileri silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla; veri sorumlusu sıfatıyla **Ludens İleri Finansal Hizmetler ve Danışmanlık Ltd. Şti.** (“Ludens” ve/veya “Şirket”) tarafından hazırlanmıştır.

### 1. Tanımlar

İlgili Terim	Tanımı
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
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 kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun/KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 ortam.
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.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.

<b>Kişisel Verilerin Yok Edilmesi</b>	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
<b>Kurum</b>	Kişisel Verileri Koruma Kurumu
<b>Kurul</b>	Kişisel Verileri Koruma Kurulu.
<b>Özel Nitelikli Kişisel Veri</b>	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.
<b>Periyodik İmha</b>	Kanun'da yer alan kişisel verilerin işleme 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.
<b>Veri Sahibi/İlgili Kişi</b>	Kişisel verisi işlenen gerçek kişi.
<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
<b>Yönetmelik</b>	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.
<b>Açık Rıza</b>	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

## 2. İlkeler

Şirket tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilmektedir:

- 2.1. Kişisel verilerin güvenliğinin sağlanması, silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'un 4. maddesinde sayılan ilkeler ile 12. maddesi kapsamında alınması gereken ve işbu Politika'nın 5.2. maddesinde belirtilen teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politika'ya uygun olarak hareket edilmektedir.
- 2.2. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Ludens tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.
- 2.3. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı seçilmektedir. Ancak, İlgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.

- 2.4. Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Ludens tarafından re'sen veya Kanun'un 13. maddesine istinaden İlgili Kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından Ludens'e başvurulması halinde;
- 2.5. Kişisel verileri işleme şartlarının tamamen ortadan kalkmış olması halinde; iletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve İlgili Kişiye belirttiği iletişim kanalından bilgi verilmektedir.
- 2.6. Kişisel verileri işleme şartları tamamen ortadan kalkmış ve talebe konu kişisel verilerin üçüncü kişilere aktarılmış olması halinde; bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.
- 2.7. Kişisel veri işleme şartlarının tamamının ortadan kalkmamış olması halinde; söz konusu talep Ludens tarafından Kanun'un 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanmak suretiyle reddedilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

### 3. Saklama ve İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

Veri sahiplerine ait kişisel veriler, Şirket tarafından özellikle: (i) Ticari faaliyetlerin sürdürülebilmesi, (ii) Hukuki yükümlülüklerin yerine getirilebilmesi ve (iii) çalışan haklarının ve yan haklarının planlanması ve ifası için Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aşağıdaki gibidir:

- *Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,*
- *Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,*
- *Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanması zorunlu olması,*
- *Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,*
- *Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,*
- *Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.*

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Şirket tarafından resen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

- *Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası sebebiyle gerekli olması hali,*
- *Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,*
- *Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,*
- *Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,*

- *İlgili kişinin, Kanun'un 11. maddesindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,*
- *Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,*
- *Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.*

#### 4. Saklama ve İmha Süreleri

Şirket tarafından Kanun ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha sürelerinin tespitinde aşağıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır:

- Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Anılan sürenin sona ermesi akabinde veri hakkında aşağıdaki madde kapsamında işlem yapılır,
- Söz konusu kişisel verinin saklanmasına ilişkin olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;
  - Kişisel veriler, Kanun'un 6. maddesinde yer alan tanımlama baz alınarak, kişisel veriler ve özel nitelikli kişisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının Şirket nezdindeki önem derecesine göre belirlenir.
  - Verinin saklanmasının Kanun'un 4. maddesinde belirtilen ilkelere uygunluğu örneğin; verinin saklanmasında Şirket'in meşru bir amacının olup olmadığı sorgulanır. Saklanmasının Kanun'un 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
  - Verinin saklanmasının Kanun'un 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.

Şirket tarafından tespit edilen saklama, imha ve periyodik imha sürelerine, işbu Politika'nın Ek-1'inde yer alan İmha Süreleri ekinde ulaşabilirsiniz. Saklama süresi dolan kişisel veriler, işbu Politika'nın ekinde yer alan imha süreleri çerçevesinde, 6 (altı) aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak anonim hale getirilir veya imha edilir. 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.

## 5. Kişisel Verilerin Saklanması ve İmhasına İlişkin Usuller, Teknik ve İdari Tedbirler

### 1. Saklama Ortamları

Şirketimizin yükümlülüklerini yerine getirebilmesi, bir hakkın tesisi için, veri işleminin zorunlu olması, müşteri hizmetleri, tüketici hakları ve diğer imkânlardan istifade edebilmeniz ve/veya bunlarla ilgili ticari mali hukuki sorumluluk ve yükümlülüklerin yerine getirilebilmesi, Şirketimizin güvenliğinin sağlanması veya Şirketimizin meşru amaçları için kişisel verilerinizin işlenmesine gerek olması halinde toplanılacak olan kişisel veriler kaydedilmektedir.

Veri sahiplerine ait kişisel veriler, Ludens tarafından aşağıda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

#### • Elektronik Ortamlar

- File Server
- Cloud (bulut tabanlı) Server
- .....
- ..... (Muhasebe/bordro programı)

#### • Fiziksel Ortamlar

- Birim Dolapları
- Arşiv
- .....
- .....

### 2. Teknik ve İdari Tedbirler

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla Kanun'un 12. maddesindeki ilkeler çerçevesinde, Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

#### a. İdari Tedbirler:

Şirket idari tedbirler kapsamında;

- i. *Kişisel Veri İşleme Envanterini hazırlar.*

- ii. Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- iii. İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- iv. Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- v. Veri sorumlusu adına kişisel veriyi işlenen kurum ve kuruluşlar ile veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- vi. Kişisel veri içeren kâğıt ortamındaki evrakların, sunucuların, yedekleme cihazlarının, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin artırılmasına ilişkin önlemleri alır.
- vii. Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- viii. Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- ix. Kişisel verilerin bulunduğu ortama göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmasını sağlar ve bu ortamlara yetkisiz giriş çıkışları engeller.

#### **b. Teknik Tedbirler:**

Şirket idari tedbirler kapsamında;

- i. Kurulan sistemler kapsamında gerekli iç kontrolleri yapar.
- ii. Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür.
- iii. Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar.
- iv. Verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi ihtimallere istinaden alınan yedeklere sadece sistem yöneticisinin erişebilmesini sağlar.
- v. Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda delillerin toplanmasını ve güvenli bir şekilde saklanmasını sağlar.
- vi. Verilerin bulunduğu cihazların arıza veya bakım nedeniyle servis gibi üçüncü kurumlara gönderilmesi gerekmesi halinde, teknik olarak mümkün ise gönderilmeden önce kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılmasını sağlar.
- vii. Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolünü sağlar.
- viii. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.
- ix. Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulmasını (log kayıtları gibi) sağlar.
- x. Kişisel verilerin yok edilmesini, geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlar.
- xi. Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur.

Şirket tarafından yürütülen süreç ve kişisel veri bazında yukarıda izahı yapılan idari ve teknik tedbirlerin hangilerinin benimsendiğine ilgili Kişisel Veri İşleme Envanterinden ulaşabilirsiniz.

**c. Teknik ve İdari Tedbirlerden Sorumlu Personel:**

Kişisel veri saklama ve imha sürecinde yer alan personelin unvanları, birimleri ve görev tanımları işbu Politika'nın EK-2'sinde yer alan listede yer almaktadır.

**6. Kişisel Verilerin İmha Usulleri**

Şirket tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde Şirket tarafından re'sen yahut İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilecektir.

**3. Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri**

Şirket tarafından kişisel verilerin silinmesi ve yok edilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır

**a. Kişisel Verilerin Silinmesi:**

- i. **Yazılımdan Güvenli Olarak Silme:** Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.
- ii. **Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi;** merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.
- iii. **Diğer yollar;** Kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.
  - *Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,*
  - *Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.*
- iv. **Uzman Tarafından Güvenli Olarak Silme:** Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

v. **Kâğıt Ortamında Bulunan Kişisel Verilerin Karartılması:** Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir

b. **Kişisel Verilerin Yok Edilmesi:**

- i. **De-manyetize Etme:** Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.
- ii. **Fiziksel Yok Etme:** Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kâğıt ve mikrofiş ortamındaki verilerin yok edilmesi de başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.
- iii. **Üzerine Yazma:** Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

### 1. Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri

Şirket tarafından kişisel verilerin anonim hale getirilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır: Şirket tarafından bu yöntemlerden birisi gerçekleştirilerek anonim hale getirilmesi istenen kişisel veri anonimleştirilir. KVKK'nin 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

- i. **Değişken Çıkartma:** Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden "yüksek dereceli betimleyici" olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir.
- ii. **Kayıtları Çıkartma:** Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademedede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.



- iii. **Bölgesel Gizleme:** Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır. Örneğin, şirketin futbol takımının yedek listesinde olan ilgili veri sorumluları arasında yalnızca bir kişi 65 yaşında ise yaş, cinsiyet ve sağlık durumu yönünden futbol oynayabilecek olup olmadığı bilgisinin birlikte saklandığı bir veri kümesinde 'Yaş:65' yerine 'Bilinmiyor' yazılması veya bu kısmın boş bırakılması anonimleştirmeyi sağlayacaktır.
- iv. **Alt ve Üst Sınır Kodlama:** Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.
- v. **Genelleştirme:** Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.
- vi. **Gürültü Ekleme:** Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.
- vii. **Veri Değiş Tokuşu:** Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.

## 7. Politikanın Yürürlüğe Sokulması, İhlal Durumları ve Yaptırımlar

İşbu Politika tüm çalışanlara duyurularak yürürlüğe girecek ve yürürlüğü itibariyle tüm iş birimleri, danışmanlar, dış hizmet sağlayıcıları ve kişisel veri işleyen herkes için bağlayıcı olacaktır.

Çalışanların politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın amiri tarafından bağlı bulunan bir üst amire bildirilecektir.

Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır.

Kişisel veriler politikanın 4. maddesinde belirtilen hususlar dikkate alınarak aşağıdaki tabloda belirtilen süreler boyunca saklanarak, süre sonunda ise anonim hale getirilecek veya yok edilecektir:

**EK-1**  
**İMHA SÜRELERİ**

Süreç	Saklama Süresi	Yasal Dayanak
Şirket Ortakları ve Yönetim Kurulu Üyelerine ait bilgiler (Huzur Hakkı kâr payı ödemeleri vb)	10 yıl	6102 Sayılı Türk Ticaret Kanunu

Süreç	Saklama Süresi	Yasal Dayanak
Şirket Ortakları ve Yönetim Kurulu Üyelerine ait bilgiler (Pay Defterinde yer alan kişisel veriler)	Süresiz	6102 Sayılı Türk Ticaret Kanunu
Genel Kurul İşlemleri	10 yıl	6102 Sayılı Türk Ticaret Kanunu
İşe alım evrakları ile Sosyal Güvenlik Kurumuna bildirim gerçekleştirilen; hizmet süresine esas özlük verileri	10 yıl	5510 Sayılı sosyal Sigortalar Kanunu ve ilgili mevzuat
İş Kanunu kapsamında saklanan veriler (ör. Çalışan memnuniyeti, performans kayıtları vs.)	10 yıl	6098 Sayılı Borçlar Kanunu
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (sağlık raporları vs.)	15 yıl	6331 Sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Yönetmeliği
SGK mevzuatı kapsamında tutulan veriler	10 yıl	5510 Sayılı sosyal Sigortalar Kanunu ve ilgili mevzuat
İş kazası/meslek hastalığına ilişkin bir talepte/davada kullanılabilecek dokümanlar	10 yıl	6331 sayılı İş Sağlığı ve Güvenliği Kanunu
Kamera Kayıtları	30 Gün	Sektörel Teamül
Fatura- Gider Pusulası-Makbuz gibi belgelerle işlenen veriler	5 yıl	213 Sayılı vergi usul kanunu
Muhasebe ve Finansal İşlemlere İlişkin tüm kayıtlar	10 yıl	6102 Sayılı Türk Ticaret Kanunu ve 213 Sayılı Vergi Usul Kanunu
Şirket İnternet Ağını Kullanılması, işlem trafik bilgileri	2 yıl	5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun
Sözleşmeden Kaynaklı İlişkilerde İşlenen Kişisel Veriler	10 yıl	6098 Sayılı Türk Borçlar Kanunu
Müşteri İşlemleri	10 yıl	6098 Sayılı Türk Borçlar Kanunu
Müşteri verileri	10 yıl	6102 Sayılı Türk Ticaret Kanunu

Şirket'in ilgili kişisel veriyi kullanma amacı sona ermedi ise, ilgili mevzuat gereği ilgili kişisel veri için öngörülen saklama süresi tabloda yer alan sürelerden fazla ise veya ilgili konuya ilişkin dava zamanaşımı süresi kişisel yerinin tabloda yer alan sürelerden fazla saklanmasını gerektiriyorsa, yukarıdaki tabloda yer alan süreler uygulanmayabilecektir. Bu halde kullanım amacı, özel mevzuat veya dava zamanaşımı süresinden hangisi daha sonra sona eriyor ise, o süre uygulama alanı bulacaktır.

**EK-2**  
**PERSONEL GÖRE LİSTESİ**

PERSONEL	GÖREV	SORUMLULUK
<b>İK Müdürü</b>	İK Departmanı - Kişisel veri saklama ve imha politikası uygulama sorumlusu	<i>Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi</i>
<b>Bilgi İşlem Müdürü</b>	Bilgi Teknolojileri Departmanı - Kişisel veri saklama ve imha politikası uygulama sorumlusu	<i>Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi</i>
<b>Muhasebe Müdürü</b>	Mali İşler Departmanı - Kişisel veri saklama ve imha politikası uygulama sorumlusu	<i>Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi</i>
<b>İdari İşler Müdürü</b>	İdari İşler Departmanı - Kişisel veri saklama ve imha politikası uygulama sorumlusu	<i>Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi</i>
.....	.....	.....
.....	.....	.....