



## Kişisel Verilerin Korunması Hakkında Kanun Kapsamında Kişisel Veri Saklama ve İmha Politikası

### 1. Amaç ve Kapsam

Kişisel Verileri Saklama ve İmha Politikası (“**Politika**”), veri sorumlusu olarak Duruel tarafından (“**Şirket**”) gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket olarak temel prensibimiz; hizmet alan kişilere, çalışanlara, çalışan adaylarına, hizmet sağlayıcılara, ziyaretçilere ve ilgili diğer üçüncü kişilere ait kişisel verilerin Türkiye Cumhuriyeti Anayasası, uluslararası sözleşmeler ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (“**Kanun**”) ve diğer ilgili mevzuatlara uygun olarak işlenmesidir. Bu kapsamda ilgili kişilerin hak kaybına uğramaması ve haklarına etkin bir şekilde kullanması öncelik olarak belirlenmiştir.

İşbu hazırlanan Kişisel Verileri Saklama ve İmha Politikası, Kanun, 28.10.2017 tarih ve 30224 Sayılı Resmi Gazetede yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik (Yönetmelik) ve diğer mevzuat hükümlerine uyumlu şekilde hazırlanmıştır.

### 2. Tanımlar

<b>Alıcı Grubu</b>	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
<b>Açık Rıza</b>	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
<b>Anonim Hale Getirme</b>	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
<b>Çalışan</b>	Şirket personeli.
<b>Elektronik Ortam</b>	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
<b>Elektronik Olmayan Ortam</b>	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
<b>Hizmet Sağlayıcı</b>	Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
<b>İlgili Kişi</b>	Kişisel verisi işlenen gerçek kişi.
<b>Komite</b>	Şirket tarafından, kişisel verilerin korunması mevzuatına uygunluğun sağlanması, muhafazası ve sürdürülmesi kapsamında kurum bünyesinde gerekli koordinasyonu sağlayacak olan birim.

<b>Kişisel Veri Koruma Görevlisi</b>	Mevzuat uyarınca yükümlülüklerini yerine getiren Şirket'e, veri işleyene ve Şirket çalışanlarına bilgi veren ve tavsiyede bulunan, veri sorumlusu veya veri işleyen kişisel verilerin korunması ile ilgili politikalarının yanı sıra kişisel veri işlemede yer alan çalışanların bilinçlendirilmesi ve eğitilmesi ve ilgili denetimlerin mevzuata uygunluğunu takip edilmesinden sorumlu kişidir. <i>Veri koruma görevlisi veri işleme faaliyetlerinde danışılması gereken konularda yetkili kişilerle irtibatı sağlamaktadır.</i>
<b>İlgili Kullanıcı</b>	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 kişiler.
<b>Departman</b>	Şirket bünyesinde yer alan departmanlar.
<b>İmha</b>	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
<b>Kanun</b>	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
<b>Kayıt Ortamı</b>	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.
<b>Kişisel Veri</b>	Kişiyi belirli veya belirlenebilir kılan her türlü bilgi.
<b>Kişisel Veri İşleme Envanteri</b>	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 envanter.
<b>Kişisel Verilerin İşlenmesi</b>	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
<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 veriler.
<b>Periyodik İmha</b>	Kanunda 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>Politika</b>	Kişisel Verileri Saklama ve İmha Politikası.

<b>Veri İşleyen</b>	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
<b>Veri Kayıt Sistemi</b>	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
<b>Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)</b>	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
<b>Yönetmelik</b>	28 Ekim 2017 tarihli Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

### 3. Kayıt Ortamları

Aşağıdaki tablo, Şirket tarafından saklanan kişisel verilerin hangi ortamlarda kayıt altına alındığını göstermektedir. Şirket tarafından saklanan kişisel veriler, niteliğine ve hukuki durumuna göre en uygun kayıt ortamında saklanır.

Veri Kayıt Ortamı	Açıklama
<b>Elektronik Ortamlar</b>	<ul style="list-style-type: none"> <li>• Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, dosya paylaşım, vb.)</li> <li>• Yazılımlar (Ofis yazılımları, İtranet Portal, ERP yazılımları, Netsis“ vb.)</li> <li>• Bilgi güvenliği cihazları (Güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.)</li> <li>• Bilgisayarlar (Masaüstü, dizüstü)</li> <li>• Mobil Cihazlar (Telefon, tablet vb.)</li> <li>• Optik diskler (CD, DVD vb.)</li> <li>• Çıkartılabilir bellekler (USB, hafıza kartı vb.)</li> </ul>
<b>Elektronik Olmayan Ortamlar</b>	<ul style="list-style-type: none"> <li>• Kâğıt</li> <li>• Manuel veri kayıt sistemleri (Not defterleri, dosyalar, klasörler vb.)</li> </ul>

### 4. Sorumluluk ve Görev Dağılımları

Yönetmeliğin 6. maddesinin f bendi uyarınca kişisel verilerin saklanmasında ve imha süreçlerinde yer alan kişilerin unvanlarının, görevlerinin ve birimlerinin belirtilmesi gerektiği düzenleme altına alınmıştır. Bu kapsamda kişisel verilerin hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi, kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla veri güvenliği, saklama ve imha süreçlerinin yönetimi, teknik ve idari tedbirlerin alınması konularında Şirket bünyesinde bulunan kişilere ait unvanları, görev ve birimleri belirtilmiştir.

Unvan	Görev Tanımı
<b>Kişisel Veri Koruma Komitesi</b>	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmesi süreçlerinin yürütülmesinden, değerlendirilen taleplerin karara bağlanmasından ve saklama süreçlerinin yürütülmesinden sorumludur.

**Şirket Kişisel Veri Koruma Görevlisi**

İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Koruma Komitesi'ne raporlanmasından; Kişisel Veri Koruma Komitesi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Komite'nin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Komite'ye raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

## 5. Saklama ve İmhaya İlişkin Açıklamalar

Şirket hizmet sağladığı kişilere sağlamış olduğu ticari hizmet kapsamında ilgili kişilere ait kişisel verileri Kişisel Verilerin Korunması Kanunu'nun belirtmiş olduğu hususlara uygun olarak ve Şirket'in Kişisel Verilerin Korunması ve İşlenmesi Politikasına uygun olarak işlemektedir. Şirket ilgili kişilere ait kişisel verileri işbu politikada belirtilen kayıt ortamlarında saklamakla beraber yine bu politikada belirtilen şekilde imha etmektedir.

Ayrıca Şirket yanında çalışan personellere ait kişisel verileri, Kişisel Verilerin Korunması Kanunu'nun belirtmiş olduğu hususlara uygun olarak ve Şirket'in Kişisel Verilerin Korunması ve İşlenmesi Politikasına uygun olarak işlemektedir. Şirket ilgili kişilere ait kişisel verileri işbu politikada belirtilen kayıt ortamlarında saklamakla beraber yine bu politikada belirtilen şekilde imha etmektedir.

Şirket bünyesinde sunulan hizmetler sebebiyle toplanan kişisel veriler, Kişisel Verilerin Korunması Kanunu'nun 5. ve 6. Maddelerinde belirtilen kişisel veri işleme şartlarından birine veya birkaçına dayalı olarak saklanmaktadır. Söz konusu kişisel veri işleme şartı sona erdiğinde veya ilgili kişinin Şirket'e başvurusu üzerine, (Şirket'in riayet etmesi gereken diğer yasal süreler ve yükümlülükler kontrol edildikten sonra) kişisel veriler silinmekte, imha edilmekte veya anonim hale getirilmektedir.

### 5.1. Saklamayı Gerektiren Hukuki Sebepler

Şirket, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir.

Bu kapsamda kişisel veriler;

- ✓ 4857 sayılı İş Kanunu,
- ✓ 6098 sayılı Türk Borçlar Kanunu,
- ✓ 6102 Sayılı Türk Ticaret Kanunu,
- ✓ 3308 sayılı Mesleki Eğitim Kanunu,
- ✓ 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu
- ✓ 6698 Sayılı Kişisel Verilerin Korunması Kanunu
- ✓ 5237 Sayılı Türk Ceza Kanunu
- ✓ 3218 Sayılı Serbest Bölgeler Kanunu
- ✓ İş Sağlığı ve Güvenliği Yönetmeliği gereğince öngörülen saklama süreleri kadar saklanmaktadır.

### 5.2. Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri belirli amaçlar doğrultusunda saklamaktadır.

Bu kapsamda amaçlar aşağıda sayılmıştır:

- ✓ Acil Durum Yönetimi Süreçlerinin Yürütülmesi

- ✓ Araç Pasavan Pulu Başvuru Süreçlerinin Yürütülmesi
- ✓ Bilgi Güvenliği Süreçlerinin Yürütülmesi
- ✓ Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- ✓ Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- ✓ Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
- ✓ Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- ✓ Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
- ✓ Denetim / Etik Faaliyetlerinin Yürütülmesi
- ✓ Eğitim Faaliyetlerinin Yürütülmesi
- ✓ Erişim Yetkilerinin Yürütülmesi
- ✓ Faaliyetlerin Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- ✓ Faaliyetlerin Mevzuata Uygun Yürütülmesi
- ✓ Finans Ve Muhasebe İşlerinin Yürütülmesi
- ✓ Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
- ✓ Fiziksel Mekan Güvenliğinin Temini
- ✓ Görevlendirme Süreçlerinin Yürütülmesi
- ✓ Hukuk İşlerinin Takibi Ve Yürütülmesi
- ✓ İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- ✓ İletişim Faaliyetlerinin Yürütülmesi
- ✓ İnsan Kaynakları Süreçlerinin Planlanması
- ✓ İş Faaliyetlerinin Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
- ✓ İş Faaliyetlerinin Yürütülmesi / Denetimi
- ✓ İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- ✓ İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
- ✓ Kullanıcı Hesaplarının Oluşturulması
- ✓ Lojistik Faaliyetlerinin Yürütülmesi
- ✓ Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- ✓ Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
- ✓ Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- ✓ Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
- ✓ Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- ✓ Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
- ✓ Organizasyon Ve Etkinlik Yönetimi
- ✓ Pazarlama Analiz Çalışmalarının Yürütülmesi
- ✓ Performans Değerlendirme Süreçlerinin Yürütülmesi
- ✓ Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
- ✓ Risk Yönetimi Süreçlerinin Yürütülmesi
- ✓ Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
- ✓ Sözleşme Süreçlerinin Yürütülmesi
- ✓ Stratejik Planlama Faaliyetlerinin Yürütülmesi
- ✓ Talep / Şikayetlerin Takibi
- ✓ Taşınır Mal Ve Kaynakların Güvenliğinin Temini
- ✓ Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- ✓ Ücret Politikasının Yürütülmesi
- ✓ Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- ✓ Veri Sorumlusu Operasyonlarının Güvenliğinin Temini

- ✓ Yabancı Personel Oturma ve Çalışma İzni İşlemleri
- ✓ Yatırım Süreçlerinin Yürütülmesi
- ✓ Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
- ✓ Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- ✓ Yönetim Faaliyetlerinin Yürütülmesi
- ✓ Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

### 5.3. Kişisel Verilerin İmha Edilmesini Gerektiren Haller

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,
- ✓ Kişisel Verilerin Koruması Kanunu'nun 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- ✓ İlgili mevzuatlarda yer alan saklama sürelerinin sona ermesi,
- ✓ Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- ✓ Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kurumu'na şikâyetle bulunması ve bu talebin Kurum tarafından uygun bulunarak ilgili kişisel verinin imhasının talimatlandırılması durumlarında Şirket tarafından silinir, yok edilir veya anonim hale getirilir.

## 6. Kişisel Verilerin Güvenli Şekilde Saklanması, Hukuka Aykırı İşlenmesi Ve Erişiminin Önlenmesi İçin Alınmış Teknik Ve İdari Tedbirler

Şirket, kişisel verilerin güvenli bir şekilde saklanmasını sağlamak amacıyla kişisel verilerin tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır. Şirket aldığı teknik ve idari tedbirler ile verilerin hukuka aykırı olarak işlenmesini ve yetkisiz kişilerce erişilmesini önlemektedir.

Bu kapsamda Şirket Kişisel Verilerin Korunması Kanunu'nun 12. Maddesinde yer alan veri güvenliğine ilişkin yükümlülüklerini yerine getirmekte olup, kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemekte, kişisel verilerin muhafazasını sağlamaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

### 6.1. İdari Tedbirler

Şirket, kişisel verilerin saklandığı tüm ortamların, ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- ✓ Çalışanlar için veri güvenliğine yönelik disiplin düzenlemeleri mevcuttur.
- ✓ Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

- ✓ Kişisel verilerin işlenmesi, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
- ✓ Gizlilik taahhütnameleri yapılmaktadır.
- ✓ İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- ✓ Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- ✓ Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- ✓ Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- ✓ Kişisel veri güvenliğinin takibi yapılmaktadır.
- ✓ Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- ✓ Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- ✓ Kişisel veriler mümkün olduğunca azaltılmaktadır.
- ✓ Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- ✓ Mevcut risk ve tehditler belirlenmiştir.
- ✓ Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.

## 6.2. Teknik Tedbirler

Şirket, kişisel verilerin saklandığı tüm ortamların, ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- ✓ Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- ✓ Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- ✓ Çalışanlar için yetki matrisi oluşturulmuştur.
- ✓ Gerekliğinde veri maskeleyme önlemi uygulanmaktadır.
- ✓ Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- ✓ Güncel anti-virüs sistemleri kullanılmaktadır.
- ✓ Güvenlik duvarları kullanılmaktadır.
- ✓ Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- ✓ Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- ✓ Şifreleme yapılmaktadır.
- ✓ Veri kaybı önleme yazılımları kullanılmaktadır.
- ✓ Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

## 7. Kişisel Verileri İmha Teknikleri

Şirket, Kişisel Verilerin Koruması Kanunu ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikası'na uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Politika'da belirtilen sürelerin sona ermesi ile re'sen siler, yok eder veya anonim hale getirir. Şirket tarafından kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

### 7.1. Silme Yöntemleri

Kişisel verilerin silinmesi, kişisel verilerin kurum içerisinde ilgisi olan kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler silinir.

<b>Fiziksel Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri</b>	
<b>Karartma</b>	Fiziksel ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep, kullanılarak görünmez hale getirilmesi şeklinde yapılır.
<b>Sunucularda Yer Alan Kişisel Veriler</b>	
<b>Erişim yetkisini kaldırarak silme</b>	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılır ve silme işlemi yapılır.

## 7.2. Yok Etme Yöntemleri

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler yok edilir.

<b>Fiziksel/Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
<b>Fiziksel yok etme</b>	Matbu ortamda tutulan belgeler evrak imha makineleri ve imha makinelerinin çalışma sistemine benzer yöntemler ile tekrar bir araya getirilemeyecek şekilde yok edilir.
<b>Yerel Dijital Ortamda ve Sunucularda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
<b>Fiziksel yok etme</b>	Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.
<b>De-manyetize etme (degauss)</b>	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
<b>Üzerine yazma</b>	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
<b>Erişim yetkisini kaldırarak yok etme</b>	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılır ve bir daha ulaşılamayacak şekilde yok etme işlemi yapılır
<b>Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
<b>Yazılımdan güvenli olarak silme</b>	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

### 7.3. Anonimleştirme Yöntemleri

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler anonim hale getirilir.

<b>Fiziksel/Matbu Ortamda Tutulan Kişisel Veriler İçin Anonim Hale Getirme Yöntemleri</b>	
<b>Değişkenleri Çıkarma</b>	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabilmesi gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.

<b>Genelleştirme</b>	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.
<b>Alt Ve Üst Sınır Kodlama / Global Kodlama</b>	Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir. Aynı kategori içinde kalan değerler birleştirilir.
<b>Mikro Birleştirilme</b>	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
<b>Veri Karma Ve Bozma</b>	Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.
<b>Dijital Ortamda/Sunucularda/Bulut Ortamın Tutulan Kişisel Veriler İçin Anonim Hale Getirme Yöntemleri</b>	
<b>Maskeleme (şifreleme, simge kullanma, bulanıklaştırma, karıştırma, geçersizleştirme)</b>	Veri maskeleme kişisel verilere yetkisiz kişiler tarafından erişilmesini engellemek amacıyla anlaşılabilir hale getirilmesidir. Bu yöntem kurumda bulunan gizli ve hassas bilgilerin kurum içerisine ve kurum dışına sızmasını, kötü niyetli kişilerce ele geçirilmesini engellemek amacıyla kullanılmaktadır. Veri maskelemede veri formatı değiştirilmez sadece değerler değiştirilir ancak bu değişim herhangi bir şekilde tespit edilmeyecek ve geri döndürülmeyecek şekilde yapılmaktadır. Ayrıca kimlerin hangi verilere ulaşabileceği belirlenerek sadece yetkisi olan kişilerin görmesi gereken bilgileri görmesi ve diğer bilgilerin maskelenmesi sağlanır.

## 8. Kişisel Verileri Saklama ve İmha Süreleri

Şirket tarafından, faaliyetler kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- ✓ Süreçler bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Şirket Kişisel Veri İşleme Envanterinde,
- ✓ Veri kategorileri bazında saklama süreleri VERBİS'e kayıta,
- ✓ Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Şirket tarafından güncellemeler yapılır.

Veri Kategorisi	Saklama Süresi	İmha Süresi
<b>Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Eğitim Bilgisi</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

<b>Finans</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Fiziksel Mekan Güvenliği</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Görsel Kayıtlar</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Hukuki İşlem</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İletişim</b>	Süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İşlem Güvenliği</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Kimlik</b>	Süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Lokasyon</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Mesleki Deneyim</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Müşteri İşlem</b>	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Özlük</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Sağlık</b>	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

## 9. Veri İmha Süreleri

Şirket Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası, diğer hazırladığı politikalar ve işbu Politika uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanun'un 13'ncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

✓ Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Şirket'in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Başvuru ve Yanıt Prosedürüne uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.

✓ Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

## 10. Periyodik İmha Süreleri



Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, her yıl Haziran ve Aralık aylarında saklama süresi dolmuş fiziksel ve dokümanların periyodik imha işlemi gerçekleştirilir

## **11. Politikanın Yayınlanması, Saklanması ve Güncellenmesi**

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayınlanır. Kurumsal internet sayfasında kamuya açıklanır. Basılı kağıt nüshası da Kişisel Veri Koruma Komitesince ve Kişisel Veri Koruma Görevlisince dosyada saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

## **12. Uyum ve Değişiklikler**

Şirket, mevzuat hükümleri gereği ya da Şirket politikası gereği kişisel verilerin saklanması ve imha politikasında değişiklik yapma hakkına sahiptir. İşbu Politika ..../.... tarihinde yayınlanmış olup herhangi bir değişiklik yapılmamıştır.

**Duruel A.Ş.**