

# ATAY MAKİNA SAN. VE TİC. LTD. ŞTİ.

## KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

### 1. Amaç ve Kapsam

Kişisel Verileri Saklama ve İmha Politikası (Politika), Atay Makina Sanayi ve Ticaret Limited Şirketi (Şirket) tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerinde uygulanacak usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket ortakları, çalışanlar, stajyerler, çalışan ve stajyer adayları, ziyaretçiler, tedarikçi çalışanları, ürün veya hizmet alan ya da almaya aday kişi ve kurum çalışanları ile diğer üçüncü kişilere (ilgili kişi) ait kişisel veriler Şirket tarafından T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun), Kişisel Verileri Koruma Kurulu (Kurul) kararları ve diğer mevzuata uygun olarak işlenmektedir.

İlgili mevzuat ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (Yönetmelik) uyarınca, Şirketin işlemekte olduğu kişisel verilerin saklanması ve işlenmesini gerektiren sebeplerin ortadan kalkması halinde hukuka uygun olarak imhasına ilişkin iş ve işlemler, işbu Politikaya uygun olarak gerçekleştirilir. Bu kapsamda, Şirketin faaliyetleri çerçevesinde işlenen kişisel veriler, bu kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik tüm faaliyetlerde işbu Politika uygulanır.

### 2. Kısaltma ve Tanımlar

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Alıcı grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar

Hizmet Sağlayıcı	Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
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 kişiler
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kanun	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 veri işleme envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 detaylandıkları envanter
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Kişisel verilerin silinmesi	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Kişisel verilerin yok edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi

Kurul	Kişisel Verileri Koruma Kurulu
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler
Periyodik imha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
Politika	Kişisel Verileri Saklama ve İmha Politikası
Sicil	Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili
Şirket	Atay Makina Sanayi ve Ticaret Limited Şirketi
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

### 3. Politikanın Uygulanmasında Sorumlular ve Görev Dağılımları

İşbu Politikanın uygulanması ve kişisel verilerin saklama ve imha süreçlerinde görevli olanların unvan, birim ve görev tanımları aşağıda yer alan tabloda gösterilmektedir. Tabloda yer alan yönetici, birim yöneticisi, çalışan ve hizmet sağlayıcıların yanında, diğer tüm Şirket çalışanları ve hizmet sağlayıcılar Politikaya uygun faaliyet gösterme, alınan teknik ve idari tedbirlerin uygulanmasını sağlama, kişisel verilere hukuka aykırı olarak erişimin engellenmesi ve kişisel verilerin hukuka aykırı olarak işlenmesinin engellenmesinden sorumludur.

Unvan	Birim	Görev
Genel Müdür	Atay Makina Sanayi ve Ticaret Limited Şirketi Genel Müdürlüğü	Çalışanların ve dış hizmet sağlayıcıların politikaya uygun hareket etmesinden sorumludur.
Bilgi İşlem Sorumlusu	Bilgi İşlem Hizmet Sağlayıcısı	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulması ve düzenli olarak güncellenmesinden sorumludur.
Muhasebe ve İnsan Kaynakları Müdürü	Muhasebe ve İnsan Kaynakları Departmanı	Görevlerine uygun olarak Politikanın yürütülmesinden, görevi kapsamında işlenen kişisel verilerin saklama ve imha sürelerinin takibi ile gerekli iş ve işlemlerin yapılmasından/yaptırılmasından sorumludur.
Satın Alma ve Lojistik Müdürü	Satın Alma ve Lojistik Departmanı	Görevlerine uygun olarak Politikanın yürütülmesinden, görevi kapsamında işlenen kişisel verilerin saklama ve imha sürelerinin takibi ile gerekli iş ve işlemlerin yapılmasından/yaptırılmasından sorumludur.
İş Geliştirme ve Satış Müdürü	İş Geliştirme ve Satış Departmanı	Görevlerine uygun olarak Politikanın yürütülmesinden, görevi kapsamında işlenen kişisel verilerin saklama ve imha sürelerinin takibi ile gerekli iş ve işlemlerin yapılmasından/yaptırılmasından sorumludur.
Yönetici Asistanı	Destek Hizmetleri Birimi	Görevlerine uygun olarak Politikanın yürütülmesinden, görevi kapsamında işlenen kişisel verilerin saklama ve imha sürelerinin takibi ile gerekli iş ve işlemlerin yapılmasından/yaptırılmasından sorumludur.

#### 4. Kayıt Ortamları

Şirket faaliyetleri kapsamında işlenmekte olan kişisel verileri aşağıda yer alan tabloda gösterilen kayıt ortamlarında hukuka uygun olarak saklanmaktadır.

Elektronik Ortam	Elektronik Olmayan Ortam
Bilgisayarlar	Birim dolapları (klasör, dosya, defter vb.)
Mobil cihazlar	Arşiv odası (klasör, dosya, defter vb.)
Harici depolama aygıtları	Yönetici asistanı ve diğer asistanlarca idare edilen dolaplar (Ziyaretçi giriş defteri, sekreterlik defteri vb.)
Sunucular	
Yazılımlar	
Bilgi güvenliği cihazları	
Yazıcı, tarayıcı, fotokopi makineleri	
Güvenlik kameraları	

#### 5. Kişisel Verilerin Saklanması ve İmhasını Gerektiren Sebepler

Şirket tarafından ilgili kişilere ait kişisel veriler Kanun, Yönetmelik, Kurul kararları ve diğer mevzuata uygun olarak saklanır ve imha edilir.

##### 5.1. Kişisel Verileri Saklama Sebep ve Amaçları

Kanunun 4. maddesi gereğince kişisel verilerin saklanma sürelerinin tespitinde ilgili mevzuatta öngörülen süreler veya işleme amacının sona ermesi dikkate alınmaktadır. Şirket faaliyetleri kapsamında işlenen kişisel verilerin saklanmasına dair yükümlülükleri ve saklama sürelerini belirleyen ilgili mevzuat şöyledir:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6098 sayılı Türk Borçlar Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 4857 sayılı İş Kanunu

- 213 Sayılı Vergi Usul Kanunu
- 5434 sayılı Emekli Sandığı Kanunu
- 2828 sayılı Sosyal Hizmetler Kanunu
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik

Şirket, kişisel verileri aşağıdaki amaçlarla saklar:

- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan/Stajyer Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışanlar/Stajyerler İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Finans ve Muhasebe İşlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İnsan Kaynakları Süreçlerinin Planlanması
- İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- İş Faaliyetlerinin Yürütülmesi
- İş sağlığı ve güvenliği faaliyetlerinin yürütülmesi
- İşçi sağlığının korunması
- Kurumun Fiziksel Güvenliğinin Sağlanması
- Kurum İçerisinde ve Çevresinde Görüntü Kaydının Tutulması
- Mal / Hizmet Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Performans Değerlendirme Süreçlerinin Yürütülmesi
- Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Şirketin hukuki yükümlülüklerinin yerine getirilebilmesi
- Ürün/Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- Yönetim Faaliyetlerinin Yürütülmesi
- Ziyaretçi Kaydı Oluşturulması ve Takibi

## 5.2. Kişisel Verilerin İmhasını Gerektiren Sebepler

Şirket, faaliyetleri çerçevesinde işlediği kişisel verileri aşağıdaki sebeplerden birinin varlığı halinde imha eder. İmha işlemi kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde gerçekleştirilebilir.

- Kişisel verilerin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası
- Kişisel verilerin işlenmesini 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 Şirket tarafından kabul edilmesi
- Şirketin 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 şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

## 6. Kişisel Verileri İmha Yöntemleri

Kişisel verilerin imhasını gerektiren sebeplerden (5.2.) birinin varlığı halinde, kişisel verilerin Şirket tarafından silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir. Kişisel verilerin yer aldığı elektronik ya da elektronik olmayan ortamlardaki tüm kopyalar üzerinde bu işlemlerin uygulanması gerekir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar en az üç yıl süreyle saklanır.

### 6.1. Silme

Kişisel verilerin silinmesi işlemi ile kişisel veriler ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Kişisel verilerin silinmesinde yararlanılan yöntemler şöyledir:

- Kağıt Ortamında Bulunan Kişisel Veriler: Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünmez hale getirilmesi şeklinde yapılır.
- Merkezi Sunucuda Yer Alan Kişisel Veriler: Kişisel verilerin yer aldığı dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılmasıyla gerçekleştirilir.
- Veri Tabanlarında Bulunan Kişisel Veriler: Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinir. Bu şekilde kişisel veri, veri tabanı yöneticisi hariç hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
- Bulut Sisteminde Yer Alan Veriler: Bulut sisteminde veriler silme komutu verilerek silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığı kontrol edilir.
- Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, bu ortamlara uygun yazılımlar kullanılarak silinir ve yalnızca sistem yöneticisi tarafından erişilebilecek şekilde şifreli olarak saklanır.

## 6.2. Yok Etme

Kişisel verilerin yok edilmesi işlemi ile kişisel veriler hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilir. Kişisel verilerin yok edilmesinde yararlanılan yöntemler şöyledir:

- Fiziksel Ortamda Yer Alan Kişisel Veriler: Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma 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. Manyetik medya ve yeniden yazılabilir optik medya üzerine rastgele veriler yazılarak eski verinin kurtarılmasının önüne geçilmesi sağlanır.

- Bulut Ortamında Bulunan Kişisel Veriler: Kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.
- Arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi: İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel veriler yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir. Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanır; arızalı diğer parçalar üretici, satıcı, servis gibi üçüncü kurumlara gönderilir. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemler alınır.

### **6.3. Anonim Hale Getirme**

Kişisel verilerin anonim hale getirilmesi işlemi ile kişisel veriler başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilir.

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 uygulanması sonucunda elde edilen veriler belirli bir kişiyi tanımlayamaz niteliğe kavuşturulur.

## **7. Kişisel Verileri Saklama ve İmha Süreleri**

Şirket, saklama süreleri sona eren ve böylece silme, yok etme veya anonim hale getirme yükümlülüğü ortaya çıkan kişisel verileri, bu tarihi takip eden ilk periyodik imha işleminde siler, yok eder veya anonim hale getirir.

Şirket tarafından kişisel verileri saklanan bir kişinin Şirkete başvurarak verilerin silinmesini veya yok edilmesini talep etmesi halinde:

- a. Şirket, kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.
- b. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.
- c. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Kanun m. 13/3 uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Süreç	Saklama Süresi	İmha Süresi
Çalışan/stajyer özlük dosyası oluşturma (kimlik ve iletişim bilgileri, işe giriş bildireleri, prim/hizmet belgeleri, disiplin ve performans belgeleri, şirket içi eğitim bilgileri, adli makamlarla yazışmalar, adli sicil kaydı)	İşten ayrılmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan/stajyer özlük dosyası oluşturma (askerlik, bordro, tazminat, yıllık izin)	İşten ayrılmasından itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan/stajyer özlük dosyası oluşturma (özgeçmiş, diploma, transkript, meslek içi eğitim)	İşten ayrılmasından itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler	İşten ayrılmasından itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan adaylarına/stajyer adaylarına ait veriler	Başvurunun kabul edilmediği tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarikçi/ürün veya hizmet alan kurum yetkili ve çalışanlarına ait veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Potansiyel tedarikçi/ürün veya hizmet alan kurum	İş ilişkisi kurulmayacağı kesinleşmesinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

yetkili ve çalışanlarına ait veriler		
Fiziksel mekan güvenliği (kamera kayıtları, ziyaretçi kaydı)	Kamera kaydının alınmasından itibaren 90 gün, ziyaretçi kaydının oluşturulmasından itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem güvenliği (çalışanlar ve çevrimiçi ziyaretçilere ait bilgiler)	İşlemin gerçekleşmesinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sekreterlik kayıtları	Kaydın gerçekleştirilmesinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Diğer veriler	İlgili mevzuatta öngörülen süre	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

## 8. Kişisel Verilerin Saklanması ve İmhasına İlişkin Teknik ve İdari Tedbirler

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Şirket tarafından alınan teknik ve idari tedbirler aşağıda listelenmiştir.

### 8.1. Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yöntemi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleyme yöntemi uygulanmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

## **8.2. İdari Tedbirler**

- Kişisel veri güvenliği politika ve prosedürleri uygulanmaktadır.
- İlgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Özel nitelikli kişisel verilerin işlendiği ve saklandığı ortamların güvenlik önlemleri alınmaktadır.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler uygulanmaktadır.
- Yetkisiz giriş çıkışlar engellenmektedir.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar uygulanmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

## 9. Periyodik İmha Süresi

Şirket, 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. Periyodik imha süresi Yönetmelik m. 11 gereğince 6 ay olarak belirlenmiştir ve her yılın Haziran ve Aralık aylarında gerçekleştirilir.

## 10. İlgili Kişinin Hakları

Kanun'un 11. maddesinde düzenlenen ve aşağıda aktarılan haklarınızı, Şirketimize [www.ataymakina.com](http://www.ataymakina.com) adresinde yer alan Başvuru Formu aracılığıyla ve kimliğinizi tespit edici belgeleri de sağlayarak kullanabilirsiniz. Başvuru formunun Kanun'un 13. ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5. maddelerine uygun olarak ilgili formda yer alan başvuru adresi veya e-posta adresi kullanılarak Şirketimize iletilmesi gerekmektedir. Bu doğrultuda form ve kimliğinizi tespit edici belgeleri yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da önceden şirketimize bildirmiş olduğunuz ve sistemimizde kayıtlı bulunan elektronik posta adresinizi kullanmak suretiyle iletebilirsiniz.

Şirketimiz başvurunuzda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kişisel Verileri Koruma Kurulu tarafından belirlenen tarifedeki ücret alınabilir. Başvurunuz sonrasında talebiniz değerlendirilerek kabul veya gerekçesi açıklanarak reddedilir; talebinize dair cevap ilgili kişiye yazılı olarak veya elektronik ortamda bildirilir. Başvuruda yer alan talebin kabul edilmesi hâlinde talebin gereği yerine getirilir. Başvurunun veri sorumlusu olarak Şirketin hatasından kaynaklanması halinde alınan ücret ilgiliye iade edilir.

Kanun'un 11. maddesi kapsamında haklarınız:

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) Kanun'un 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

## 11. Diğer Hükümler

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, Şirket web sitesinde kamuya açıklanır. Politika, Şirket web sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. Değişiklikler güncelleme tablosunda gösterilir ve web sitesinde yayınlanmasının ardından yürürlüğe girer.

## GÜNCELLEME TABLOSU

TARİH	MADDE/MADDELER	AÇIKLAMA