KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1- AMAÇ

İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KV Kanunu") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") dahil KV Kanununun ikincil düzenlemeleri, Kişisel Verileri Koruma Kurulunun kararları (tamamı birlikte "KVK Mevzuatı") uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin veri sorumlusu sıfatıyla İkinci Plan Otomotiv ve Ticaret A.Ş. ("Şirket") tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

2- KAPSAM

İşbu Kişisel Veri Saklama ve İmha Politikası Şirket bünyesinde kişisel verileri işleyen herhangi bir sürece dahil olan tüm departmanları, çalışanları ve 3. tarafları kapsamaktadır.

Şirket çalışanlarına, çalışan adaylarına, stajyerlere, ürün ve hizmet alanlara, potansiyel müşterilere, ortaklara, ziyaretçilere, tedarikçilere ve diğer üçüncü kişilere ait tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerine ve bu verilerin saklanmasına ve imhasına ilişkindir.

Şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

3- İLKELER

Şirket, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

Şirket, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde KV Kanunu ve ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politika düzenlemelerine uygun hareket etmektedir.

Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından resen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Şirket, Kanun ve ilgili mevzuatta düzenlenen kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçmektedir.

İlgili Kişinin talebi halinde, uygun yöntem seçilecek ve talepler tebliğ tarihinden itibaren en geç 30 (otuz) gün içerisinde gerekçesi ile İlgili Kişiye açıklanacaktır.

İlgili Kişinin talebine konu verilerin üçüncü kişilere aktarılmış olması durumunda, talep verilerin aktarıldığı üçüncü kişiye bildirilecektir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması ve imha işleminde hazır bulunan kişiler (unvan, birim ve görev tanımı olmak üzere), imha yöntem, tarih ve saatin belirtilmesi ile kayıt altına alınması temin edilecektir.

Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından "Kişisel Veri İmha Protokolü"nde listelenmekte, kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler saklı kalmak üzere 3 (üç) yıl süreyle saklanmaktadır.

4- SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Şirketimiz bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız uyarınca, burada belirtilen amaçlarla işlenmekte ve yine ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süreler saklanmaktadır.

Bu kapsamda saklamayı gerektiren işleme amaçları şunlardır:

a- İnsan kaynakları süreçlerini yürütmek
b- Kurumsal iletişimi sağlamak
c- Şirket güvenliğini sağlamak
d- İstatistiksel çalışmalar yapabilmek
e- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
f- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
g- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
h- Yasal raporlamalar yapmak
i- Çağrı merkezi süreçlerini yönetmek
j- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek
k- Şirket hukuk işlerinin icrası/takibini yapmak
l- Fiziksel mekân güvenliğinin temini ve ziyaretçi kayıtlarının oluşturulması

5- SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirkette, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

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

6- İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re'sen şirket tarafından silinir ya da yok edilir:

a- Kişisel verinin hukuka aykırı olarak işlendiğinin tespit edilmiş olması,
b- Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması,
c- Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
d- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
e- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu Şirket tarafından veya Kişisel Verileri Koruma Kurumu tarafında kabul edilmesi,
f- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

7- SORUMLULUK VE GÖREVLER

İşbu Politika tüm kişisel veri işleyen kişilere Madde 15'te belirtilen şekillerde duyurularak yürürlüğe girecek ve yürürlüğü itibariyle tüm çalışanlar, birimleri, hizmet sağlayıcıları ve kişisel veri işleyen herkes için bağlayıcı olacaktır. Şirketin tüm çalışanları ve birimleri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması ve kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi konusunda sorumlu birimlere destek verecektir.

Tüm iş birimleri kendi yürüttükleri süreçlerle ilgili olarak KVK Kanunu, ilgili mevzuat ve Kurul Karalarına uyum amacıyla kişisel verilerin işlenmesi, saklanması ve imha edilmesi için gerekli tedbirleri almaktan sorumludur. Çalışanların politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğunda olacaktır.

Politikaya aykırı davranış tespit edildiğinde tespit eden kişi derhal Kişisel Veri Komisyonuna bilgi verecektir.

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

Kişisel Veri Komitesi, uyum süreçlerini koordine etmek ve kişisel verilerin işlenmesi, saklanması ve imha edilmesi için gerekli önlemlerin alınmasını sağlamakla Kanun ve ilgili mevzuat uyarınca şirketin yükümlülüklerini takip ve koordine ederek gerekli tedbirlerin alınmasından, birim çalışanlarının eğitilmesinden, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde sorumludur.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıda gösterilmiştir.

UNVANI	**BİRİMİ**	**GÖREVİ**
Tüm Çalışanlar	Tüm Birimler	KVK Mevzuatı, Şirket içi Politikalar ve Prosedürler ve bunlarda düzenlenen veri güvenliğini sağlamaya dönük olarak teknik ve idari tedbirlerin uygulanmasına destek vermek ve sorumlu birimlerle işbirliği içinde çalışmakla sorumludur.
KVK Komitesi Koordinatörü (İdari İşler)	Kişisel Veri Komitesi	• Çalışanların politikaya uygun davranmasından, • Çalışanların bu Politika kapsamında eğitimlerinden, • Periyodik imha süreçlerinin takibi; verilerin muhafaza süreleri boyunca saklanması, süre bitiminde imha edilmesinden, • İlgili Kişi taleplerinin incelenmesinden, değerlendirilmesinden, yanıtlanmasından ve kararı uyarınca yerine getirilmesinden; • Saklama ve imha süreçlerinin kayıtlarının tutulmasından; sorumludur.
KVK Komite Üyesi (İdari İşler)		• Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden; • Şirketin tüm birimleri dahilinde süreçlerin saklama sürelerinin belirlenmesinden sorumludur.
KVK Komite Üyesi (Bilgi İşlem)	Bilgi İşlem Müdürlüğü	• Verilerin saklanması ve imhası süreçlerinde gerekli teknik ve idari tedbirlerin alınması ve takibinden; • Periyodik imha ve ilgili kişi talebi neticesinde silme, yok etme veya anonim hale getirme işlemlerinin KVK Mevzuatına ve bu Politikaya uygun şekilde gerçekleştirilmesi; • Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sağlanmasından sorumludur.

8- KAYIT ORTAMLARI

Kişisel veriler, şirket tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

ELEKTRONİK ORTAMLAR	
I. Sunucular E-Posta: Microsoft Exchange Yedekleme: Yedekleme Ortamları Metin girmek için burayı tıklatın. **II. Yazılımlar** Microsoft Office (ofis yazılımları v.b.) Metin girmek için burayı tıklatın. **III. Bilgi güvenliği cihazları** Güvenlik Duvarı: Antivirüs: Saldırı Tespit ve Engelleme Sistemi: Log Kayıtları Metin girmek için burayı tıklatın.	**IV. Bilgisayarlar (masaüstü, dizüstü)** Metin girmek için burayı tıklatın. **V. Mobil cihazlar** (telefon, tablet, navigasyon vb.) **VI. Optik diskler (CD, DVD vb.)** **VI. Taşınabilir bellekler (USB, Hafıza Kartı vb.)** **VIII. Yazıcı, tarayıcı, fotokopi makinesi**

FİZİKSEL ORTAMLAR	
I. Fiziki kayıt ortamları yazılı, basılı, görsel: Belgeler Formlar	**II. Diğer Ortamlar** Birim Dolapları Arşiv

9- TEKNİK TEDBİRLER

Şirket, Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun olarak imha edilmesi için **asgari olarak** aşağıda belirtilen teknik ve idari tedbirleri alınmaktadır:

a- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır
b- Anahtar yönetimi uygulanmaktadır
c- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır
d- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır
e- Erişim logları düzenli olarak tutulmaktadır
f- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır
g- Saldırı tespit ve önleme sistemleri kullanılmaktadır
h- Şifreleme yapılmaktadır
i- Veri kaybı önleme yazılımları kullanılmaktadır
j- Güncel anti-virüs sistemleri kullanılmaktadır
k- Güvenlik duvarları kullanılmaktadır
l- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır
m- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir
n- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

10- İDARİ TEDBİRLER

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıdadır:

a- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır
b- Çalışanlar için yetki matrisi oluşturulmuştur
c- Mevcut risk ve tehditler belirlenmiştir
d- KVler mümkün olduğunca azaltılmaktadır
e- KV içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır
f- KV içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır
g- KV içeren ortamların güvenliği sağlanmaktadır
h- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır
i- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır

Yukarıda sayılanlar asgari tedbirleri teşkil etmekte olup bunların da dahil olduğu, Şirketin uyguladığı tam kapsamlı 'TEKNİK VE İDARİ TEDBİRLER' **KV Organizasyon Envanteri.xls** dokümanında güncel haliyle kaydedilmektedir.

11- KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

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

Kişisel veriler aşağıda belirtilen yöntemlerle silinir.

VERİ KAYIT ORTAMI	SİLİNME YÖNTEMİ
Sunucular	Sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortam	Veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Bulut	
Fiziksel ortam	Evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkeple çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir medya	Sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

12- KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel veriler aşağıda belirtilen yöntemlerle yok edilir.

VERİ KAYIT ORTAMI	YOK EDİLME YÖNTEMİ

Elektronik ortam	İlgili üreticinin önerdiği yöntemler ya da fiziksel yok etme veya üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir.
Fiziksel ortam	Evrak imha makinelerinde geri birleştirilemeyecek şekilde küçük parçalara bölerek yok edilir.
Optik ya da manyetik medya	Yakılarak veya doğranarak 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
Taşınabilir medya	Fiziksel yok etme veya üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir.

13- KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

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, alıcı veya alıcı grupları tarafından geri döndürme ve 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.

⚠ Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemleri yalnızca ilgili kişisel verilerin **veri sorumlusu nezdinde ve veri işleyenler nezdinde** herhangi bir kopyasının (ör. yedekleme) dahi kalmaması durumunda tamamlanmış olacaktır. Bu yüzden her imha işleminde tüm ortamlarda kopyaları da tespit edilmeli ve imha edilmelidir ve veri işleyenlerin de aynı işlemleri gerçekleştirmeleri sağlanmalıdır.

14- SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bunun haricinde "KV Organizasyon Envanteri.xls" Excel çalışma kitabında yer alan saklama ve imha süresi tablosu esas alınır. Genel bir oryantasyon verisi olarak aşağıda gösterilen süreler uygulanır.

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler	İş ilişkisinin bitimini müteakip 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha günü
İş Kanunu kapsamında saklanılan veriler	İş ilişkisinin bitimini müteakip 10 yıl	
Bordrolama	İş ilişkisinin bitimini müteakip 10 yıl	
İş Kanunu Kapsamında Saklanan Özlük Dosyasına İlişkin Veriler	İş İlişkisinin sona ermesinden itibaren 10 Yıl	
Personel mahkeme/adliye taleplerinin cevaplandırılması	İş ilişkisinin bitimini müteakip 10 yıl	
Çalışanların Kişisel Verilerinin Yer Aldığı Ortamlara İlişkin Yaptığı Erişimlerin Log Kayıtları	En Az 2 Yıl Olmak Suretiyle İş Davalarına Konu Olabilmesi Sebebiyle 10 Yıl	
Eğitim kayıtlarının dosyalanması	Eğitimin düzenlenmesinin ardından 10 yıl	
SGK Mevzuatı kapsamında tutulan veriler	İş İlişkisinin sona ermesinden itibaren 10 Yıl	
İş Başvurusu/Staj Başvurusu/ Başvuru Kabul Edilmediği Takdirde Adaya İlişkin Veriler	Red kararından itibaren 3 ay	
Adayın Açık Rıza Beyanı	Red kararından itibaren 1 yıl	

durumunda		
Çevrim içi Ziyaretçilere İlişkin Trafik Bilgileri	Kaydedilmesinden itibaren 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha günü
Şirket Faaliyetleri Uyarınca, Saklanması Gereken Ticari Defterlerde Yer Alan Kişisel Veriler	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha günü
Tedarikçilere İlişkin Kişisel Veriler	Hukuki ilişki sona erdikten sonra 10 Yıl	
Muhasebe ve Finans Kayıtları	10 Yıl	
Sözleşmeler	Sözleşmenin Sona Ermesinden İtibaren 10 Yıl	
E-postalar ve şirket içi yazışmalar	10 Yıl	
Kişisel Veri İmha Kayıtları	Kaydedilmesinden itibaren 3 yıl	
Güncelliğini yitirmiş Politikalar ve Prosedürler	Yürürlükten kaldırılmasından itibaren 5 yıl	

Yukarıda belirtilen süreler uygulanmakla beraber, veri sorumlusunun meşru menfaatinin olduğu durumlarda, işlenme amacının ve ilgili kanunlarda belirtilen sürelerin de sona ermesine rağmen veri sahiplerinin temel hak ve özgürlüklerine zarar vermemek kaydıyla kişisel veriler, Borçlar Kanunu'nda düzenlenen genel zamanaşımı süresinin (on yıl) sona ermesine kadar saklanabilecektir. Bahsi geçen zamanaşımı süresinin sona ermesinin ardından kişisel veriler, politika belgesinde belirlenen prosedüre göre silinecek, yok edilecek yahut anonim hale getirilecektir.

15- PERİYODİK İMHA SÜRESİ

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması ve muhafaza yükümlülüğü bulunmaması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen saklama süresinin bitimini takip eden ilk periyodik imha zamanında re'sen siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri her yıl Haziran ve Aralık aylarında olmak üzere her 6 (altı) ayda bir tekrar eder.

16- POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, fiziki ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında ilan edilir. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

17- YÜRÜRLÜK

Politika, şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın iptal edilmiş versiyonu ve en az 5 yıl süre ile şirket tarafından saklanır.