

## KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

### 1. POLİTİKANIN AMACI

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a (Kanun) dayalı olarak çıkarılmış olan ve 30224 sayılı Resmi Gazete'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Yönetmelik) 5. ve 6. maddeleri gereği kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi için ŞİRKET genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

### 2. POLİTİKANIN KAPSAMI

Politika, şirket nezdinde tutulan, Kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri, tüm şirket çalışanlarını, yöneticilerini, danışmanlarını ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerini, dış hizmeti sağlayıcılarını ve şirketin sair hukuki ilişkiye girdiği gerçek ve tüzel kişileri kapsamaktadır. Politika Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri kapsamaktadır. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.

### 3. TANIMLAR

**Anonim Hale Getirme:** Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

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

**Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

**Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

**Kişisel Verilerin Silinmesi:** Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

**Kişisel Verilerin Yok Edilmesi:** Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

**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 verilerini,

**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 işlemini,

**Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

#### 4. POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI

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 kayıt ortamı kapsamına girer.

Kişisel veriler elektronik ortamlarda (sunucular, yazılımlar, kişisel bilgisayarlar, mobil cihazlar, çıkartılabilir bellekler) ve elektronik olmayan ortamlarda (kağıt, manuel veri kayıt sistemi, yazılı, basılı, görsel ortamlar) saklanmaktadır.

#### 5. KİŞİSEL VERİLERİ KORUMA KOMİTESİ'NİN GÖREV VE YETKİLERİ

**5.1.** Kişisel Verileri Koruma Komitesi Politikanın ilgili iş birimlerine duyurulmasından ve gereklerinin şirket birimlerince yerine getirilmesinin takibinden sorumludur.

**5.2.** Kişisel Verileri Koruma Komitesi kişisel verilerin korunmasına ilişkin mevzuat değişiklikleri, Kurulun düzenleyici işlemleri ile kararları, mahkeme kararları veya süreç, uygulama ve sistemlerdeki değişiklikler gibi durumları ilgili iş birimlerinin takip etmesi ve gerekiyorsa iş süreçlerini güncellemeleri için gerekli duyuruları ve bildirimleri yapar,

**5.3.** Kişisel Verileri Koruma Komitesi; Kanun ve ikincil düzenlemeleri ile Kurulun kararları ve düzenlemeleri, mahkeme kararları ve sair yetkili makamların kararlarının ve/veya taleplerinin incelenmesi, değerlendirilmesi, takibi ve sonuçlandırılmasına yönelik süreçleri belirler ve ilgili birimlere duyurur.

#### 6. KİŞİSEL VERİLERİN SAKLANMASI VEYA İMHASINI GEREKTİREN SEBEPLER VE İŞLENME ŞARTLARININ ORTADAN KALKMASI DURUMUNDA YAPILACAKLAR

**6.1.** Şirket bünyesinde işlenen kişisel veriler mevzuatta hüküm bulunması durumunda bu süre kadar muhafaza edilir. İşlenen kişisel veriler; İş Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Türk Borçlar Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, İş Sağlığı ve Güvenliği Kanunu, Vergi Usul Kanunu ve diğer vergi mevzuatı, Avukatlık Kanunu ve diğer ilgili mevzuatta belirtilen süreler kadar saklanmaktadır. Her bir kişisel veri işleme süreci için saklama süresinin ne olduğu kişisel veri işleme envanterinde ayrıntılı olarak yer almaktadır.

Şirket bünyesinde işlenen kişisel verilerin saklanmasını gerektiren amaçlar şunlardır; çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi, sözleşmelerin imzalanması, insan kaynakları süreçlerinin yürütülmesi, çalışanlar için yan menfaat süreçlerinin yürütülmesi, iş faaliyetlerinin yürütülmesi/denetimi, iş sağlığı ve güvenliğinin sağlanması, iş başvurularının değerlendirilebilmesi, çalışanların çalışma becerisinin geliştirilmesi, mal hizmet satın alım süreçlerinin yürütülmesi, sözleşme süreçlerinin yürütülmesi, mal hizmet üretim ve operasyon süreçlerinin yürütülmesi, reklam çalışmalarının yapılması, satış sonrası destek sürecinin yürütülmesi, pazarlama faaliyetlerinin yürütülmesi, finans ve muhasebe işlerinin yürütülmesi, mal ve hizmet satış süreçlerinin yürütülmesi, faaliyetlerin mevzuata uygun yürütülmesi, hukuk işlerinin takibi ve yürütülmesi, mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi.

Şirketimiz tarafından işlenen kişisel verilerinizin imhasını gerektiren sebepler şunlardır; işleme ve saklama amacının ortadan kalkması, kişisel verinin açık rızaya dayalı olarak işlendiği durumda açık rızanın geri alınması, ilgili kişinin kişisel verisinin imha edilmesi talebinin şirketimiz tarafından kabul edilmesi, ilgili kişinin kişisel verisinin imha edilmesi talebinin şirketimizce reddedilmesi üzerine bu talebin Kurul tarafından kabul edilmesi, kişisel verilerin saklanması için öngörülen azami sürenin ortadan kalmış olması.

**6.2.** Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işleme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir. Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

**6.3.** Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi şirket birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç altı aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildiri üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır.

**6.4.** Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu

politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır.

**6.5.** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

**6.6.** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

**6.7.** Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden şirkete başvurarak kendisine ait kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini talep ettiğinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Bu talep, başvuru tarihinden itibaren en geç otuz gün içinde sonuçlandırılır ve ilgili kişiye Müşteri Hizmetleri Birimi aracılığıyla bilgi verilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, ilgili veri sahibi iş birimi bu durumu derhal aktarım yapılan üçüncü kişiye bildirir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

**6.8.** Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, kişisel veri sahiplerinin verilerinin silinmesi veya yok edilmesine yönelik talepleri şirket tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı ilgili kişiye en geç 30 gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

**6.9.** Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara yönlendirilecektir.

## **7. POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR**

**7.1.** İşbu Politika tüm çalışanlara duyurularak yürürlüğe girecek ve yürürlüğü itibarıyla tüm iş birimleri, danışmanlar, dış hizmet sağlayıcıları ve sair şirket nezdinde kişisel veri işleyen herkes için bağlayıcı olacaktır.

**7.2.** Şirket çalışanlarının 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. Aykırılığın önemli boyutta olması halinde ise üst amir tarafından vakit kaybetmeksizin Kişisel Verileri Koruma Komitesi'ne bilgi verilecektir.

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

**7.4.** Politika gereklerinin yerine getirilmesi için şirket tarafından; gerekli tüm güvenlik önlemleri alınmaktadır.

## **8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI**

Şirket içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette şirket nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerinde bulunması durumunda, söz konusu veri bilgi sistemlerinden sorumlu birimler tarafından saklanacaktır.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak ilgili bilgi sistemleri bölümlerince yapılacaktır.

Kişisel verilerin saklama ve imha süreçlerinde yer alacak kişiler ve sorumlulukları şu şekildedir;

<b>UNVAN</b>	<b>BİRİM</b>	<b>GÖREV</b>
Şirket Yetkilisi	Şirketi Yönetimi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
Genel Müdür	Şirket Yönetimi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi Güvenliği Firması	Şirketin Bünyesinde Bir Birim Olmayıp Sözleşme Çerçevesinde Hizmet Alınmaktadır.	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Bilgi İşlem, Destek Hizmetleri, Hukuk Hizmetleri, İnsan Kaynakları, Muhasebe, Satış	Diğer Birimler	Görevlerine uygun olarak politikanın yürütülmesinden sorumludur.

Birimleri.

## 9. TEKNİK VE İDARİ TEDBİRLER

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

**Alınan teknik tedbirler şu şekildedir:** Ağ güvenliği ve uygulama güvenliği sağlanmaktadır, bilgi teknolojileri sistemlerinin bakımları periyodik olarak yaptırılmaktadır, güncel anti virüs sistemleri kullanılmaktadır, güvenlik duvarları kullanılmaktadır, kullanılmayan yazılımlar silinmektedir, yazılım güncellemeleri yapılmaktadır, işyeri sistemlerine kullanıcı adı ve şifre ile girilmektedir, Log kayıtları tutulmaktadır, düzenli olarak yedekleme yapılmaktadır, özel nitelikli kişisel veriler şifrelenmektedir, personelin verilere erişim yetkisi görev kapsamı ile sınırlandırılmıştır, kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır, kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır, kişisel veri içeren ortamların fiziksel ve dijital güvenliği sağlanmıştır, şifreleme yapılmaktadır, siber güvenlik önlemleri alınmıştır.

**Alınan idari tedbirler şu şekildedir:** çalışanların niteliği ve teknik bilgi/becerisinin geliştirilmesi, kişisel verilerin hukuka aykırı işlenmenin önlenmesi, kişisel verilere hukuka aykırı erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri ve ilgili mevzuatlar hakkında eğitimler verilmekte, çalışanlara gizlilik sözleşmeleri imzalatılmakta, görevden ayrılan personelin verilere erişim yetkisi derhal kaldırılmaktadır, güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü uygulanmakta, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmekte, kurum içi periyodik ve rastgele denetimler yapılmakta ve çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

## 10. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel veriler aşağıda açıklaması yapılan yöntemlerle silinmektedir;

**Sunucularda yer alan kişisel veriler:** sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

**Elektronik ortamda yer alan kişisel veriler;** elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

**Fiziksel ortamda yer alan kişisel veriler;** fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

**Taşınabilir ortamlarda bulunan kişisel veriler;** flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

## 11. KİŞİSEL VERİLERİN YOK EDİLMESİ

**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.

**Dijital ortamda 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. Sunucular vb. yerlerde yer alan kişisel veriler bilgi işlem tarafından geri getirilmemek üzere yok edilir.

## 12. 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 veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

### 13. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel Verileri Saklama ve İmha Süreleri Kişisel Veri İşleme Envanterinde yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Bu süreler aşağıda verilen tabloda da ayrıca düzenleme altına alınmıştır.

İşlenen kişisel verilerin saklanması için mevzuatta öngörülen süreler var ise bu veriler mevzuatta öngörülen süre kadar saklanmak zorundadır. Bu verilere ilişkin imha işlemi ancak mevzuatta öngörülen sürelerin dolmasının ardından yapılabilir.

Kişisel verileri saklama ve imha süreleri şu şekildedir;

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Çalışan İnsan Kaynakları Süreçlerinin Yürütülmesi	İş Akdinin Sona Ermesinden İtibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Çalışan Adayı ve Stajyer İnsan Kaynakları Süreçlerinin Yürütülmesi	6 Ay	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Satış Süreçlerinin Yürütülmesi	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Muhasebe Faaliyetlerinin Yürütülmesi	Hukuki İlişkinin Sona Ermesinden İtibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Bilgi İşlem Faaliyetlerinin Yürütülmesi	3 Ay	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Hukuk Hizmetlerinin – Dava ve İcra İşlerinin Yürütülmesi	Dava ve İcra İşlemlerinin Sona Ermesinden itibaren 3 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Destek Hizmetlerinin Yürütülmesi	2 Ay	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi

### 14. PERİYODİK İMHA SÜRELERİ

Kişisel Verileri Periyodik İmha Süresi veri sahibi ilgili iş birimleri tarafından tespit ve tayin edilir; ancak her hâlükârda bu süre 6 (altı) ayı geçemez.



## 15. YÜRÜRLÜK

**15.1.** Politika yayınlanma tarihi itibari ile yürürlüğe girecektir.

**15.2.** Politikanın şirket genelinde duyurulması ve gerekli güncellemelerin yapılması Kişisel Verileri Koruma Komitesi'nin sorumluluğundadır.

