Kişisel Veri Saklama ve İmha Politikası

1.POLİTİKANIN AMACI

İşbu Kişisel Veri Saklama ve İmha Politikasının ("Politika") 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 Veser Kimyevi Maddeler A.Ş. ("Veser") nezdinde uygulanacak kurallar ile süreç ve yükümlülükleri belirlemektir.

2.POLİTİKANIN KAPSAMI

Politika; Veser nezdinde tutulan tüm Veser çalışanlarına, yöneticilerine, danışmanlarına ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerine, üçüncü şahıs mal ve hizmeti sağlayıcılarına ve Veser'in sair hukuki ve ticari ilişkiye girdiği gerçek ve tüzel kişilere ait Kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri 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 Saklama Tablosu: Kişisel verilerin VESER nezdinde tutulacağı süreleri gösteren tabloyu,

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 işlenme 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

Kişisel veriler, Veser tarafından aşağıda listelenen ortamlarda kanunlara uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (E-posta veri tabanı, web,dosya paylaşımı, yedekleme vb.) Yazılımlar (ofis yazılımları) Bilgi Güvenliği Cihazları (güvenlik duvarı, saldırı tespit ve engelleme, antivirüs vb.) Video Kaydı Kişisel Bilgisayarlar (Masaüstü,dizüstü) Mobil Cihazlar (telefon,tablet) Çıkartılabilir Bellekler (USB, Hafıza Kart vb.) Yazıcı, tarayıcı, fotokopi makinası	Kağıt Manuel Veri Kayıt Sistemi (anket formları) Yazılı, basılı görsel ortamlar

5.SAKLAMAYA İLİŞKİN AÇIKLAMALAR

Veser tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve müşteri olarak ilişkide bulunulan üçüncü kişilere ait Kişisel Veriler Kanuna uygun olarak saklanır.

A.Saklamaya İlişkin Açıklamalar

Veser, ticari, idari ve hukuki faaliyetleri çerçevesinde Kişisel Verileri ilgili mevzuatta öngörülen

veya işleme amaçlarına uygun süre kadar saklar.

A.1 Saklamayı Gerektiren Hukuki Sebepler

Veser yukarıda belirtilen faaliyetleri çerçevesinde işlediği Kişisel Verileri ilgili mevzuatlarda öngörülen süre kadar saklar. Bu kapsamda Kişisel Veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar
- Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin

- Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

B. Saklamayı Gerektiren İşleme Amaçları

Veser, yukarıda belirtilen faaliyetleri çerçevesinde işlemekte olduğu Kişisel Verileri aşağıda belirtilen amaçlar uyarınca saklar.

- Kanunlardan ve ilgili mevzuatlardan doğan yükümlülüklerin yerine getirmek,
- İnsan kaynakları prosedürünü işletmek, özlük dosyalarını oluşturmak, maaş ödemelerini yapmak,
- ISG kapsamında yükümlülüklerini yerine getirmek,
- Mahkemeler, icra daireleri, yetkili kurum ve kuruluşlarının talep ve kararlarının yerine getirmek,
- İnternet erişiminin denetim altında sağlanması, ilgili kanunlara uygunluğun sağlamak,
- Veser'in merkez ve depolarına giriş-çıkış kontrolünü ve güvenliğini sağlamak,
- Veser'in faaliyetleri çerçevesinde çalışanları, müşterileri ve/veya 3.kişilerle iletişimi sağlamak.
- Veser'in taraf olduğu sözleşmeler uyarınca edimin ifası sürecini yeri getirmek/getirtmek.
- Veser'in tabi olduğu mevzuattan kaynaklanan hukuki yükümlülüklerini yerine getirilmek,
- Veser'in ABD mevzuatına tabi hissedarlarının ve grup şirketlerinin yasal yükümlülükleri bakımından ABD mevzuatı gerekliliklerinin sağlanmak
- ABD mevzuatına uyumluluğunun sağlamak,
- Veser'in hissedarları ve iştiraklerine raporlama yapmak,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek,
- Açık pozisyon için işe alım değerlendirmesi yapılmak
- Çalışanların özel sağlık sigortasının yapmak
- Çalışanlara iş sözleşmelerinden doğan hak ve menfaatlerin sağlanmak
- Veser'in ticari işleyişi uyarınca meşru menfaatini korumak
- Ticari faaliyetler kapsamında cari hesap açmak, kredi limiti belirlemek, kredibilitenin değerlendirmek,

6.TEKNİK VE İDARİ TEDBİRLER

6.1 Teknik Tedbirler

Veser'in aldığı tedbirler aşağıda gösterilmektedir.

- Veser'in bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli

- önlemler alınmaktadır.
- Fiziken kişisel verilerin kilitli dolaplarda saklanması,
- Kişisel verilere erişebilecek çalışan sayısının sınırlandırılması,
- Erişimlerin kayıt altına alınarak uygunsuz erişimler kontrol altında tutulması,
- Silinen kişisel verilerin ilgili kullanıcılar için erişilmez ve tekrar kullanılamaz olması için gerekli tedbirlerin alınması,
- Hukuka Aykırı İşleme Tespiti Halinde İlgili Kişiye ve Kurula bildirmek için bir altyapı Oluşturulması,
- Çevresel tehditlere karşı 7/24 çalışan izleme sistemi,
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri
- güncel halde tutulmaktadır
- Elektronik Ortamlarda Güçlü Parolalar Kullanılması ve bu şifrelerin periyodik olarak değiştirilmesi,
- İzin verilen çalışanların VPN bağlantılarının şifre ile korunması,
- Kişisel Verilerin Güvenli Olarak Saklanmasını Sağlayan Yedekleme altyapısı, ISO 9001 sertifikasının alınması, (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü) zararlı yazılımları engelleyen sistemler vb. kullanılması,
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik risklerin belirlenmesi, bu riskler için uygun teknik tedbirlerin alınması, alınan tedbirlere yönelik önlemlerin sağlanması,
- Şirket internet sayfasında güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmesini kapsar.
- Veser içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama yapılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri
- kullanılmaktadır.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınmaktadır.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle aktarılmaktadır.

6.2 Veser'in İdari Tedbirleri

Veser'in işlediği Kişisel Verilere ilişkin aldığı idari tedbirler aşağıda belirtilmektedir:

- Çalışanların niteliği ve teknik bilgi/becerisinin geliştirilmesi,

- Kişisel verilere hukuka aykırı işlenmesinin ve erişilmesinin önlenmesi,
- Kişisel verilerin muhafazasının sağlanması,
- Çalışanlarla gizlilik sözleşmeleri imzalatılması,
- Çalışanlara ve kişisel verileri işlenen 3. Kişilere kişisel verileri işlenmeden önce Aydınlatma Metninin İmzalatılması,
- Şirket içi periyodik ve rastgele denetimler yapılması ve kişisel verileri hukuka aykırı olarak işlenmesinin ve kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi amacıyla çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.
- güvenlik politika ve prosedürlerini ihlal eden veser çalışanlarına yönelik uygulanacak disiplin prosedürü hazırlanmıştır
- Çalışanlarının kişisel verileri hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması amacıyla eğitimler verilmiş ve verilmektedir.
- Veser tarafından kişisel veriler işlenmeden önce ilgili kişilere aydınlatılmış açık rıza metni imzalatılmaktadır.
- Kişisel Verilerin işleme envanteri hazırlanmıştır.
- Ayrıca özel nitelikli kişisel verilere ilişkin olarak kişisel veriler için alınan idari tedbirlerin yanı sıra özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara veri güvenliği konularında düzenli eğitimler verilmekte,
- Özel Nitelikli Kişisel Verilerin İşlendiği ve saklandığı ortamların güvenlik önlemleri alınmakta, yetkisiz giriş çıkışlar engellenmekte, kağıt ortamında aktarımı gerekiyorsa evrak “gizlilik dereceli belgeler” formatında gönderilmektedir.

7. İMHA PROSEDÜRÜ

7.1. Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme 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.

7.2. Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi Veser birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç 6 (altı) aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildirimi üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır.

7.3. Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendisinde 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.

7.4. 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 3 (üç) yıl süreyle saklanır.

7.5. 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.

7.6. Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden Veser'e 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 durumda talep, başvuru tarihinden itibaren en geç 30(otuz) gün içinde sonuçlandırılır ve ilgili kişiye yazılı ya da elektronik ortamda 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.

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

7.8. Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Aksi durumda; ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara yönlendirilecektir.

8 KİŞİSEL VERİLERİN SİLİNMESİ VE YOK EDİLMESİ YÖNTEMLERİ

A) Kişisel Verilerin Silinmesi Yöntemleri

a. Elektronik Olmayan Ortamlardaki Kişisel Veriler: Fiziksel yok etme, üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir. Kâğıt Ortamlarında Bulunan Kişisel Veriler de kâğıt imha makinaları kullanılarak yok edilir. Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan Kişisel Veriler ise bulundukları ortama göre uygun yöntemlerle yok edilirler.

b.Sunucuda Yer Alan Ofis Dosyaları: İşletim sisteminde File Shredder programıyla DoD 5220-22.M yöntemi komutu ile silinir.

c. Taşınabilir Medyada Bulunan Kişisel Veriler: Uygun yazılımlarla veya silme komutuyla silinir.

d. Ofis Yazılımları: Kişisel Verilerin bulunduğu ilgili satırlar silme komutu ile silinir.

e. Elektronik Ortamda Yer Alan Kişisel Veriler: Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, ilgili ortama uygun şekilde silinir ve hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

9. POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR

9.1. İşbu Politika tüm çalışanlara duyurularak yürürlüğe girecek ve yürürlüğü itibariyle tüm iş birimleri, danışmanlar, üçüncü kişi hizmet sağlayıcıları ve sair Veser nezdinde kişisel veri işleyen herkes için bağlayıcı olacaktır.

9.2. Veser 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 Kurulu'na bildirim yapılacaktır.

9.3. Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında gerekli disiplin prosedürü uygulanacaktır.

10. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI

Veser içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette Veser 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 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.

11. KİŞİSEL VERİLERİ KORUMA KOMİTESİ'NİN GÖREV VE YETKİLERİ

11.1. Kişisel Verileri Koruma Komitesi, Politikanın ilgili iş birimlerine duyurulmasından ve gereklerinin Veser birimlerince yerine getirilmesinin takibinden sorumludur.

11.2. 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.

11.3. 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.

12. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Ek: 1'de yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Veser kişisel veri envanterinde yer alacak süreçlerin sahibi iş birimlerince, tereddüt halinde Kişisel Verileri Koruma Komitesi değerlendirmeleri de alınarak, güncellenecektir.

13. 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.

14. YÜRÜRLÜK

14.1. Politika yayınlanma tarihi itibari ile yürürlüğe girecektir.

14.2. Politikanın Veser genelinde duyurulması ve gerekli güncellemelerin yapılması Kişisel Verileri Koruma Komitesi'nin sorumluluğundadır.

EK- 1 - Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Kişisel veriler aksine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça Politikanın 6. maddesinde belirtilen hususlar dikkate alınarak aşağıdaki belirtilen süreler boyunca saklanacak, süre sonunda ise imha edilecektir:

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Üçüncü kişilerle imzalanan sözleşmeler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özlük dosyası	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan adayları iş başvuruları	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel bireysel emeklilik poliçeleri	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara araç tahsis edilmesi	İş sözleşmesi devam ettiği ve yargılama sürecinin söz konusu olması halinde yargılama süreci devam ettiği sürece	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 15 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

Kayıt/Takip/Log Sistemleri	2 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Güvenlik kamera görüntüleri	Görüntünün alındığı tarihten itibaren 8 ay	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Alacak/Borç ödeme işlemleri, müşteri bilgileri	Ticari ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Toplantı notlarının/memnuniyet anket formları/geri bildirim notlarının saklanması	2 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Her türlü doküman dosyalanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Hukuk süreci	Yargılama devam ettiği sürece ve yargılama süreci sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Reklam ve Tanıtım Faaliyetleri	Etkinlik tarihinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Pazarlama	Faaliyetten itibaren 2 yıl	Saklama süresinin bitimini

takiben

180 gün içerisinde