**KVKK KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

1. **AMAÇ**

İşbu Kişisel Veri Saklama ve İmha Politikası (“Politika”) **Otuzbir Kimya ve Sanayi Türk. Limited Şirketi** kısaca (“Şirket”) olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) ve sair mevzuat uyarınca kişisel verilerin korunması, silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin Şirket tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Kanun m.7/III’teki; *“Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir”* hükmü ve Kişisel Verileri Koruma Kurulu’nun (“Kurul”) yetki ve görevlerini düzenleyen m.22/1-e bendindeki; *“Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak”* hükmü gereğince Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik[[1]](#footnote-1) (“Yönetmelik”) hazırlanmıştır.

İşbu Politika doğrultusunda; kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, yukarıda yer verdiğimiz ulusal olarak kabul görmüş temel ilkeler çerçevesinde gerçekleştirilecektir.

1. **KAPSAM**

Politika, Şirket çalışanlarının, çalışan adaylarının, müşteri, müşteri adaylarının, tedarikçi, tedarikçi çalışanlarının, ziyaretçilerin, işbirliği içerisinde olduğumuz üçüncü kişilerin, üçüncü kişilerin çalışanlarının ve bunlarla sınırlı olmamak üzere, 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.

1. **TANIMLAR**

|  |  |
| --- | --- |
| **Anonim hale getirme:** | Kişisel verilerin, başka verilerle eleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi. |
| **Kişisel Veri:** | Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. |
| **Kişisel Verilerin Silinmesi:** | Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi. |
| **Kişisel Verilerin Yok Edilmesi:** | Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez veya tekrar kullanılamaz hale getirilmesi işlemi.  |
| **Kişisel Verilerin İmha Edilmesi:** | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi |
| **Kişisel Verilerin İşlenmesi ve Korunması Politikası:** | “www.otuzbirkimya.com” adresinden ulaşılabilecek, şirketimiz bünyesinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı, |
| **Kişisel Verilerin İşlenmesi:** | Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem. |
| **İlgili Kişi:** | Kişisel verisi işlenen gerçek kişi. |
| **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 verileri. |
| **Veri Sorumlusu:** | Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi. |
| **Periyodik İmha:** | Kanun’da yer alan kişisel verilerin işlenme 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. |

1. **KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR**

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Şirket, her halde veri sorumlusu sıfatı ile hareket etmekte ve kişisel verileri Kanun’a, Kişisel Verilerin İşlenmesi Ve Korunması Politikası’na ve işbu Kişisel Veri Saklama ve İmha Politikası’na uygun olarak işlemek ve korumaktadır.

|  |  |
| --- | --- |
| **1. Fiziksel Ortamlar:**  | * Birim Dolapları
* Arşiv
* Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)
* Yazılı, basılı, görsel ortamlar
 |
| **2. Yerel Dijital Ortamlar:** | * Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım)
* Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS)
* Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
* Kişisel bilgisayarlar (Masaüstü, dizüstü)
* Mobil cihazlar (telefon, tablet vb.)
* Optik diskler (CD, DVD vb.)
* Çıkartılabilir bellekler (USB, Hafıza Kartı vb.)
* Yazıcı, tarayıcı, fotokopi makinesi
 |
| **3. Bulut Ortamlar:** | Şirket bünyesinde yer almamakla birlikte, Şirket kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.  |

1. **TEKNİK VE İDARİ TEDBİRLER**

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK’nın 12. maddesindeki ilkeler çerçevesinde, Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

 **5.1. TEKNİK TEDBİRLER**

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

* Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
* Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
* Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
* Silinen kişisel verilerin ilgili kullanıcılar için erişilmez ve tekrar kullanılamaz olması için gerekli tedbirler alınmaktadır.
* Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar ve güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
* Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
* Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
* Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
* Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
* 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 alınması,
* Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
* Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

 **5.2. İDARİ TEDBİRLER**

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

* Saklanan kişisel verilere Şirket içi erişimi, iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
* İşlenen verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi halinde, durum en kısa sürede ilgilisine ve Kurul’a bildirilir.
* Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personelin niteliğinin geliştirilmesine yönelik olarak, kişisel verilerin hukuka aykırı işlenmesinin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması hakkında gerekli eğitimleri verir.
* Şirket içinde periyodik veya rastgele denetimler yapar.
* Şirket bünyesindeki kişisel verilere ve Şirket tarafından yürütülen faaliyetlere ilişkin olarak personele gizlilik sözleşmesi imzalatılır.
* Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin taahhütname imzalar yahut mevcut sözleşmeye eklenen hükümler ile veri güvenliğini sağlar.
* Kişisel veri işlenmeye başlanmadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilir.

 **5.3. ŞİRKET İÇİ DENETİM**

Şirket, Kanun’un 12. maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilmektedir.

Denetim sırasında ya da sair bir şekilde Şirket sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması halinde, Şirket bu durumu en kısa sürede ilgilisine ve Kurula bildirir.

1. **KİŞİSEL VERİLERİN İMHASI**

Şirket kişisel verileri ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etmektedir. Bu kapsamda, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediği tespit edilmekte, bir süre belirlenmişse bu süreye uygun davranılmakta, bir süre belirlenmemişse kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması durumunda, daha uzun süre işlenmelerine izin veren hukuki bir sebep bulunmaması halinde, kişisel veriler işbu Politika uyarınca silinmekte, yok edilmekte veya anonim hale getirilmektedir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ile ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 10 yıl süreyle saklanır.

  **6.1 KİŞİSEL VERİLERİN SİLİNME YÖNTEMLERİ**

* **Fiziksel Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri:**

**Karartma:** Matbu ortamda 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 görünemez hale getirilmesi şeklinde yapılır.

* **Yerel Dijital Ortamda ya da Bulut Ortamında Tutulan Kişisel Veriler İçin Silme Yöntemleri:**

**Yazılımdan Güvenli Olarak Silme:** Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

* Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
* Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

 **6.3. KİŞİSEL VERİLERİN YOK EDİLME YÖNTEMLERİ**

* **Fiziksel Ortamda Yer Alan Kişisel Veriler için Yok Etme Yöntemleri**

**Fiziksel yok etme:** Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

* **Optik / Manyetik Medyada Yer Alan Kişisel Veriler İçin Yok Etme Yöntemleri:**

**Fiziksel Yok Etme:** 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.

**De-manyetize Etme**: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.

**Üzerine yazma:** 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.

* **Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri**

**Yazılımdan güvenli olarak silme:** 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.

**6.4 Anonimleştirme Yöntemleri**

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

|  |  |
| --- | --- |
| **Değişkenleri çıkarma:** | 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 kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir. |
| **Bölgesel gizleme:** | Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir. |
| **Genelleştirme:** | Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir. |
| **Alt ve üst sınır kodlama / Global kodlama:** | 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. |
| **Mikro birleştirilme:** | 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. |
| Veri karma ve bozma | Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır. |

Şirket, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır.

1. **SAKLAMA VE İMHA SÜRELERİ**

 **7.1. Saklama Süreleri**

|  |  |  |
| --- | --- | --- |
| **VERİ SAHİBİ** | **VERİ KATEGORİSİ** | **VERİ SAKLAMA SÜRESİ** |
| Çalışan | İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri | Hizmet akdinin devamında ve hitamından itibaren de 10 (on) yıl müddetle muhafaza edilir. |
| Çalışan | İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri | Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10(on) yıl müddetle muhafaza edilir. |
| Çalışan | İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler | Hizmet akdinin devamında ve hitamından itibaren 10(on) yıl müddetle muhafaza edilir. |
| İş Ortağı/Çözüm Ortağı/Danışman | İş Ortağı/Çözüm Ortağı/Danışman ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri | İş Ortağı/Çözüm Ortağı/Danışmanın, Şirket ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |
| Çalışan Adayı | Çalışan adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler | Şirkete yapılan başvuru tarihinden itibaren 1 yıl süre ile saklanır. |
| Müşteri | Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareket bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri | Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |
| Müşteri | Kamera görüntüleri, araç plaka bilgisi | 2 yıl süre ile saklanır. |
| Potansiyel Müşteri | Potansiyel Müşteri ile Şirket arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları | 2 yıl süre ile saklanır. |
| Şirket’nın İşbirliği İçinde Olduğu Kurum/Firmalar (Tedarikçi, Fason Üretici, Bayi/Franchise) | Şirket’in işbirliği içinde olduğu Kurum/Firmalar ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, Şirket’in işbirliği içinde olduğu Kurum/Firma çalışanı verileri | Şirket’in işbirliği içinde olduğu Kurum/Firmaların, Şirket’le olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

 **7.2. İMHA SÜRELERİ**

Şirket, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası 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, Kanunun 13. maddesine istinaden Şirket’e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. 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 uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.
2. 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.
3. **PERİYODİK İMHA SÜRESİ**

Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 1 yıl olarak belirlemiştir. Buna göre, Şirket’te her yıl Aralık aylarında periyodik imha işlemi gerçekleştirilir.

1. **DİĞER HUSUSLAR**

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır. **Otuzbir Kimya ve Sanayi Türk. Limited Şirketi** tarafından hazırlanan işbu Politika 18.09.2020 tarihinde yürürlüğe girmiştir. Politika’da değişiklik olması durumunda, Politika’nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

1. RG.28.10.2017, S.30224 [↑](#footnote-ref-1)