

# Kişisel Veri Saklama ve İmha Politikası

## Amaç, Kapsam ve Tanımlar

### Amaç

Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7'nci maddesinin üçüncü fıkrası ile 22'nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5'nci maddesinde öngörülen yükümlülüğe istinaden veri sorumlusu olarak Enditeks Dış Ticaret Tekstil Sanayi ve Ticaret Ltd.Şti tarafından işlenen kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemleri için dayanak olması amacıyla hazırlanmıştır.

### Kapsam

Bu politika, Enditeks Dış Ticaret Tekstil Sanayi ve Ticaret Ltd.Şti' nin işleme amaçlarını ve vasıtalarını belirlediği, kurulmasından ve yönetilmesinden sorumlu olduğu dijital ya da analog veri kayıt sistemlerinde saklanan ve otomatik olan ya da olmayan yöntemlerle ilgili kişilerden elde edilen tüm kişisel veriler için uygulanır.

Enditeks Dış Ticaret Tekstil Sanayi ve Ticaret Ltd.Şti' nin veri sorumlusu kabul edildiği her türlü kişisel veri saklama ve imha faaliyetine uygulanır.

### 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

#### Anonim hâle getirme:

Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi

#### 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

#### İlgili kişi:

Kişisel verisi işlenen gerçek kişi

#### İlgili kişi grubu:

Veri sorumlularının kişisel verilerini işledikleri ilgili kişi kategorisi

#### İrtibat kişisi:

Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından

## Kişisel Veri Saklama ve İmha Politikası

---

Sicile kayıt esnasında bildirilen gerçek kişi

### **Kanun:**

24/3/2016 tarihli ve 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 işleme 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 envanter

### **Kişisel veri saklama ve imha politikası:**

Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika

### **Kişisel veri:**

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi

### **Kişisel verilerin işlenmesi:**

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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem

**Kişisel verilerin saklanması:** Kişisel verilerin elde edilmesini takiben içeriğini, değerini veya anlamını elde edilmesinden sonraki bir zamanda tekrar işleyebilmek için veri saklamaya elverişli bir ortamda kayıt edilmesi

### **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 veriler 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

### **Sicil:**

Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili

### **Veri işleyen:**

Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya

## Kişisel Veri Saklama ve İmha Politikası

tüzel kişi

### Veri kategorisi:

Kişisel verilerin ortak özelliklerine göre gruplandırıldığı veri konusu kişi grubu veya gruplarına ait kişisel veri sınıfı

### Veri kayıt sistemi:

Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi

### Veri sorumluları sicil bilgi sistemi (VERBİS):

Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi

### Veri sorumlusu:

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan Enditeks Dış Ticaret Tekstil Sanayi ve Ticaret Ltd.Şti

## Sorumluluk ve Görev

### Sorumluluk ve Görev Dağılımı

Bu politika kapsamındaki görevlerin belirlenmesinde sorumluluk dağılımı tabloda gösterilmiştir.

Unvan	Bölüm	Sorumluluk / Görev
Genel Müdür	Üst Yönetim	Çalışanların bu politikaya uymalarının sağlanmasından sorumludur
Veri Sorumlusu Temsilcisi	Muhasebe Bölümü	Bu politikanın gereklerinin belirlenmesi, günün şartlarına göre gerektiğinde güncellenmesi, uygulanmasının denetlenmesi için gerekli tedbirlerin alınmasından sorumludur.
Yöneticiler	İlgili Bölüm	Yöneticisi oldukları çalışanların politikaya uygun olarak çalışmalarının sağlanmasından sorumludur.
Çalışanlar	Tüm bölümler	Kişisel verilerin saklanması ve imhasında bu politikaya ve diğer hazırlanan prosedür ve talimatlara uygun hareket etmekle sorumludurlar.

### Görevler

Enditeks Dış Ticaret Tekstil Sanayi ve Ticaret Ltd.Şti' nin tüm bölümleri ve çalışanların görevleri:

Kişisel verilerin korunması konusunda yetkilendirilen kişi veya birimlerce, Politika, Prosedür ve talimatlar kapsamında belirlenen kurallar ile birlikte teknik ve idari tedbirlere uymak, gereği gibi uygulanması sağlamak.

Sorumlu oldukları bölüm varsa çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetlenmesi;

## Kişisel Veri Saklama ve İmha Politikası

---

Kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi

Kişisel verilere hukuka aykırı olarak işlenmesinin önlenmesi

Kişisel verilerin saklanması gerekiyorsa hukuka uygun olarak saklanmasının sağlanması amacıyla tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması ve uygulanması konusunda sorumlu birimlere yardım etmesi

### Saklama Ortamları

#### Dijital Ortamlar

Bu politika kapsamında kişisel verilerin sayısallaştırılarak saklandığı ve bilişim sistemleri tarafından işlenebildiği dijital ortamlar:

Sunucular (Üzerinde dijital kişisel veri saklanabilen ve hizmet üretmek amacıyla (veri tabanı, e-posta, etki alanı vb.)

Ağ ve bilgi güvenliği cihazları (router, firewall, switch, nac, Access point vb.)

Kişisel bilgisayarlar (Masaüstü, dizüstü vb.)

Mobil cihazlar (mobil telefon, tablet vb.)

Taşınabilir hafızalar (çıkartılabilir USB bellekler, CD/DVD, hafıza kartları)

Bulut

PDKS Cihazı ve Kart okuyucular

Görsel & İşitsel kayıt cihazları

Access Kontrol Cihazları

Biyometrik kontrol cihazları

Veri Depolama Cihazları

Log kayıt ürünleri; siem, 5651 v.b çözümler

#### Analog Ortamlar

Sayısallaştırılarak dijital ortama aktarılan ya da sayısallaştırılmayan kişisel verileri saklama amacıyla kullanılan analog ortamlar:

Form, defter gibi yazma araçları ile kişisel veri yazılabilecek veya baskı yoluyla elde edilmiş her türlü kişisel veri barındıran her türlü kâğıt

Üzerinde sayısallaştırılmadan kişisel veri saklamaya müsait kâğıt dışındaki her türlü ortam

Bir veri kayıt sisteminin parçası olmayan analog ortamlarda işlenen kişisel veriler için bu politika uygulanmaz.

### Kişisel Verilerin Saklanması

#### Saklamanın Gerekliliği

Kişisel veriler ancak saklanması gerekli olduğu durumlarda uygun olan ortamda veya ortamlarda saklanabilir. Saklama dışındaki diğer kişisel veri işlemler saklama olmadan da gerçekleştirilebiliyorsa, kişisel verilerin saklanması tercih edilemez.

Kişisel veriler, ancak Kişisel Verilerin Korunması Kanunu'nda ve diğer kanunlarda öngörülen

## Kişisel Veri Saklama ve İmha Politikası

usul ve esaslara uygun olarak saklanabilir.

Kişisel verinin saklanmasına karar verilirken

Hukuka ve dürüstlük kurallarına uyulması

Doğru ve güncel olması

Saklanma amacının belirli, açık ve meşru olması

Saklanma amacıyla bağlantılı, sınırlı ve ölçülü olması

İlkelerine uyulmalıdır:

### Kişisel Verilerin Saklanmasıdaki Hukuki Sebepler

Kişisel veriler ilgili kişinin açık rızası olmaksızın saklanamaz.

İlgili kişinin açık rızası;

Kanunlarda açıkça öngörülmesi,

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin saklanması için gerekli olması,

Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

İlgili kişinin kendisi tarafından saklanma amacına uygun amaçlar için alenileştirilmiş olması,

Bir hakkın tesisi, kullanılması veya korunması için saklamanın zorunlu olması

Veya ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için saklanması için zorunlu olması

Durumlarında aranmaz.

### Saklama Ortamlarının Belirlenmesi

Saklanması gereken kişisel verilerin saklanma ortamları belirlenirken zorunlu olan en az ortam belirlenmelidir. Kişisel verilerin elde edildiği ilk ortam saklamak için uygunsa ilk ortamdaki hali korunmalıdır. İlk hali saklanmaya uygun değilse, saklama süresi boyunca saklanmasına imkân vermiyorsa, işlenmesini zorlaştırıyorsa veya veri risk altında ise başka ortamda da saklanmasına karar verilebilir. Ortamın fiziksel özelliklerine göre kişisel verinin içeriğini en az değiştirecek biçimde saklanmalıdır. Elde edildiği ortamdaki diğer bir ortama aktarımı yapılırken verinin türü değişiyorsa bu değişimin veri üzerindeki değişikliklerin azaltılması için gerekli tedbirler alınmalıdır.

### Saklama Süresi

Kişisel verilerin saklanma süresi ilgili mevzuatta öngörülen süredir.

Mevzuatta herhangi bir süre öngörülmemişse saklama süresi belirlenirken

Kişisel verinin işleme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,

Kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,

Kişisel verinin işleme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,

## Kişisel Veri Saklama ve İmha Politikası

Kişisel verinin işleme amacına bağlı olarak saklanması yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,  
Kişisel verinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,  
Veri sorumlusunun hukuki yükümlülüğü gereği kişisel veriyi saklamak zorunda olduğu süre,  
Veri sorumlusu tarafından kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,  
Göz önünde bulundurulmalıdır.

Saklama süreleri öncelikle kişisel verilerin kategorilerinden bağımsız olarak buldukları bütünlük içinde değerlendirilmelidir. Bir evrak ya da belgede saklama süreleri birbirinden farklı birden fazla türde kişisel veri var ise evrak ya da belge için öngörülen saklama süresi, içerdiği kişisel veriler içinde en yüksek saklama süresidir.

Evrak ve belge üzerindeki kişisel verilerden saklama süreleri kanunla belirlenmiş olanlar için evrak ve belgedeki diğer kişisel verilerin saklama süreleri kabul edilemeyeceğinden saklama süreleri kanunla belirlenmiş kişisel verilerin silinmesi evrak ve belge imha edilmeden yerine getirilmelidir.

Saklama süreleri kişisel verilerin saklandıkları ortamlara göre farklılık gösterebilir. Bir kişisel veri hem dijital ortamda hem de analog ortamda saklanıyorsa, kişisel verinin saklama süresi bulunduğu analog ortamdaki diğer verilerle ilgili öngörülen saklama süresi kadardır. Kişisel verinin saklama süresi analog ortamın saklama süresinden daha uzun ise ve kişisel verinin bir kopyası dijital ortamda da bulunuyorsa saklama süresi evrakın saklama süresi kadardır. Sadece analog ortamda bulunuyorsa analog ortamın saklama süresi kişisel verinin saklama süresi kadar olur.

### Güvenlik Tedbirleri

Veri sorumlusu kişisel verilere yetkisiz kişilerin erişiminin engellenmesi, hukuka aykırı olarak işlenmesinin engellenmesi ve muhafazasının sağlanması için gerekli tedbirleri almak zorundadır. Kişisel verilerin saklandıkları ortamlara hukuka aykırı erişimin engellenmesi için alınması gereken tedbirler teknik ve idari tedbirler olarak ayrılır.

### Teknik ve İdari Tedbirler

Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

Çalışanlar için yetki matrisi oluşturulmuştur.

Erişim logları düzenli olarak tutulmaktadır.

Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.

Gerektiğinde veri maskeleyme önlemi uygulanmaktadır.

Gizlilik taahhütnameleri yapılmaktadır.

Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

Güncel anti-virüs sistemleri kullanılmaktadır.

## Kişisel Veri Saklama ve İmha Politikası

---

Güvenlik duvarları kullanılmaktadır.

İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

Kişisel veri güvenliğinin takibi yapılmaktadır.

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.

Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.

Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

Saldırı tespit ve önleme sistemleri kullanılmaktadır

Sızma testi uygulanmaktadır.

Şifreleme yapılmaktadır.

Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

Veri kaybı önleme yazılımları kullanılmaktadır.

### Kişisel Verilerin İmhası

Kişisel veriler, saklanmasını sağlayan şartların ortadan kalkması durumunda imha edilir.

Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, 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 imhanın gerçekleştirileceği zaman aralığı altı aydır.

#### 1. Kişisel Verilerin İmhasını Gerektiren Durumlar

Aşağıdaki durumlarda kişisel verilerin imhası gerekir.

#### Kurul Kararı

Kişisel verilerin işlenmesinin durdurulmasına ya da imhasına karar verilmesi durumunda diğer şartların varlığına bakılmadan kararın ilgili olduğu kişisel veriler imha edilir.

## Kişisel Veri Saklama ve İmha Politikası

---

### Açık Rızanın Geri Alınması

Kişisel veri işlemenin sadece ilgili kişinin açık rızasına bağlı olduğu durumlarda ilgili kişinin hukuka uygun bir şekilde açık rızasını geri alması durumunda başkaca bir işleme sebebinin bulunmaması durumunda kişisel veriler imha edilir.

### İşlenme Şartlarının Ortadan Kalkması

Kanun'un 5 ve 6'ncı maddelerinde öngörülen açık rıza dışındaki işlenme şartlarının ortadan kalkması durumunda kişisel veriler imha edilir.

### Saklama Süresinin Sona Ermesi

Bu politikada öngörülen saklama süresinin sona ermesi durumunda kişisel veriler silinir.

### Amacın Kalmaması

Kişisel verilerin saklanması gerektiren amaç ya da amaçların ortadan kalkması durumunda kişisel veriler imha edilir.

### İmha Yöntemleri

#### Silme

Kişisel verilerin silinmesiyle, bu verilerin tekrar hiçbir şekilde kullanılmayacak ve geri getirilemeyecek şekilde imhası amaçlanır. Kişisel veriler, kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi saklama ortamlarından geri dönüştürülemez şekilde silinir.

Elektronik ortamda olan ve silme işlemi uygulanabilecek kişisel veriler silinme işlemi ile silinir. Silme işlemi sonrasında geri getirilmesini önleyici tedbirler alınır.

Elektronik ortamda olmasına rağmen silme işlemi uygulanamayacak kişisel veriler için bulunduğu medyayı yok etme yöntemi kullanılır.

Kağıt ve benzeri fiziksel ortamda saklanan belgelerde silme işlemi kişisel verinin üstünün çıkmayacak koyu renk ile kapatılması ile gerçekleştirilir.

#### Yok Etme

Kişisel verilerin tekrar geri getirilemeyecek ve kullanılmayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi ortamların imha edilmesidir.

Dijital ortamlarda silinme işlemi gerçekleştirilebiliyorsa yok etme yöntemi kullanılmaz. Silinme işleminin gerçekleştirilemeyeceği optik ortamlarda ortamın çok küçük parçalara ayrılması yöntemi kullanılır.

#### Anonim Hale Getirme

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.

Anonim hale getirme kararı verilirken kişisel verilerin anonim hale getirilmesindeki zorluklar



## Kişisel Veri Saklama ve İmha Politikası

göz önünde bulundurulmalı ve son çare olarak anonim hale getirme tercih edilmelidir.

### İmha Süreleri

İşlenme şartları saklama sürelerinin sona ermesi ile ortadan kalkan kişisel veriler için imha süresi en fazla altı aydır.

İşlenme şartları sadece açık rızaya dayanan kişisel veriler açık rızanın ilgili kişi tarafından geri alınması durumunda 30 gün içinde imha edilir. İşlenme şartı sadece açık rıza olan ancak açık rızanın geri alınmasının dışında bir sebeple imhası öngörülen kişisel veri için imha süresi altı aydır.

İmha edilmesi konusunda Kurul kararı bulunan kişisel veriler için imha süresi 15 gündür.

### Periyodik İmha

Öngörülen imha süresi periyodik imha zaman diliminden önce biten kişisel veriler periyodik imha zamanı beklenmeden imha edilirler. İmha süresi 6 ay ya da daha uzun olan kişisel veriler periyodik imha zamanında imha edilirler.

Periyodik imha süresi altı aydır. Periyodik imha, imhası gereken kişisel verilerin türlerine ve sayılarına göre bir haftalık süreye yayılabilir. Periyodik imha her yılın Temmuz ve Ocak aylarının ilk haftası gerçekleştirilir.

### İmha Sırasında Tutulması Gereken Kayıtlar

Kişisel verilerin imhası sırasındaki işlemler kayıt altına alınır. İmha zamanı, imhanın periyodik olup olmadığı, imha edilen kişisel verilerin belirlenmesinde kullanılan kriterler, imha otomatik bir işlem değilse imhaya katılanların kimlikleri, imha edilen ortamlar ve kişisel veri türleri, imha işleminin sonucu ve imha süreci ile ilgili bilgi notları dijital ortamda ya da kağıt ortamında kayıt altına alınır. Varsa imha sürecine katılanlar ile paylaşılır.

Bu kayıtlar 3 yıl süre ile saklanır.

### Politikada Düzenlenmeyen Durumlar

Politikada düzenlenmeyen veya Politikanın uygulanması sonucu ortaya çıkabilecek ihtilaflarda başvurulması gereken mevzuat:

6698 sayılı Kişisel Verilerin Korunması Kanunu

28.10.2017 tarihli Resmi Gazete’de yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik

30.12.2017 tarihli Resmi Gazete’de yayınlanan Veri Sorumluları Sicili Hakkında Yönetmelik  
Kişisel verilerin saklanması atıfta bulunulan hukuki sebeplerin yer aldığı Kanun, yönetmelik ve diğer mevzuat

### Politikanın Duyurulması ve Saklanması

Politika çalışanlara mail yoluyla duyurulur.

Politika Yönetim Sistemleri bölümü tarafından saklanır.

## Kişisel Veri Saklama ve İmha Politikası

### Politikanın Güncellenmesi

Politika her yıl bir kez gözden geçirilir ve yapılması gereken değişikliklerin tespiti durumunda güncellenir. Ayrıca kişisel veri işleme envanterinde yapılan değişikliklerin politikanın güncellenmesini gerektirmesi durumlarda politika güncellenir.

### Politikada Yapılan Güncellemeler

Aşağıdaki tabloda Politikada yapılan güncellemeler ve tarihleri gösterilir.

### Saklama ve İmha Süreleri Tablosu

SÜREÇ ADI	SAKLAMA SÜRESİ	İMHA SÜRESİ
Çalışan Personel Özlük Hakları Yönetim Süreci	Çalışma sonrası 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Sağlığı ve Güvenliği Süreçleri	Çalışma sonrası 15 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Eğitim Kayıtları	İş Güvenliği Mesleki Eğitim Kayıtları 15 YIL diğerleri 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Üçüncü kişilerle imzalanan sözleşmeler	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Toplantı Notlarının/memnuniyet anket Formları/geri bildirim notlarının saklanması	Etkinliğinin sona ermesini takiben 2 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Güvenlik Kameraları Kayıtları	3 AY	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sevkiyat Kayıtları (Kantar,nakliye, Boşaltma, İrsaliye vb)	İşlem tarihinden itibaren 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul ve Yönetim Kurulu İşlemleri	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	Ortaklıktan yada üyelikten ayrıldıktan sonra 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıtları (Sistem ve Uygulamalar)	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Süreçleri	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Satın Alma Süreçleri ve Sözleşmeleri	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Satış Süreçleri ve Sözleşmeleri	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Pazarlama Faaliyeti Süreçleri	10 YIL	Saklama süresinin bitimini takip

## Kişisel Veri Saklama ve İmha Politikası

		eden ilk periyodik imha süresinde
Hukuki İşlem Süreçleri	Süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Tarih	Değişiklik	Sebebi
18.09.2020	Birinci sürüm hazırlandı	İlk hazırlandığı halin duyurulması