



**ANKARA BÜYÜKŞEHİR BELEDİYESİ**

**PORTAŞ PROJE İNŞAAT TAAHHÜT ASFALT SANAYİ VE  
TİCARET ANONİM ŞİRKETİ**

**KİŞİSEL VERİ SAKLAMA  
ve  
İMHA POLİTİKASI**

## İçindekiler

A. KAPSAM.....	3
B. TANIMLAR.....	3
C. AMAÇ VE KAPSAM .....	3
D. KAYIT ORTAMLARI .....	4
E. KİŞİSEL VERİLERİN İMHASINI GEREKTİREN DURUMLAR.....	4
F. KİŞİSEL VERİLERİN İMHASI.....	5
G. KİŞİSEL VERİLERİN İMHA YÖNTEMLERİ VE SÜRECİ.....	6
H. SAKLAMA VE İMHA SÜRELERİ.....	6
J. POLİTİKA'DA YAPILACAK DEĞİŞİKLİKLER .....	7
K. POLİTİKA'NIN YÜRÜRLÜK TARİHİ.....	8

## A. KAPSAM

1. İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"); Ankara Büyükşehir Belediyesi PORTAŞ Proje İnşaat Taahhüt Asfalt San. ve Tic. A.Ş. 'nin ("Şirket") kişisel veri işlediği süreçlere dâhil olan tüm şirket müdürlük, birim ve çalışanları ile üçüncü tarafları kapsamaktadır.
2. İşbu Politika; Şirket'in kişisel veriler üzerinde uygulayacağı tüm saklama ve imha faaliyetlerini kapsamaktadır.
3. İşbu Politika sadece kişisel verilerin imha ve saklama işlemleri için uygulanacaktır.
4. Kanun, Yönetmelik veya sair mevzuatın kısmen veya tamamen değiştirilmesi, tadil edilmesi, güncellenmesi veya yürürlükten kaldırılması durumunda Şirket, Politikayı yeni Kanun, Yönetmelik veya mevzuata uyumlu olacak şekilde güncelleyerek değiştirecektir.

## B. TANIMLAR

İşbu Politikanın uygulanmasında kullanılan kavramlar aşağıda yer verilen anlamları ifade eder;

<b>Alıcı grubu</b>	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişilerin oluşturduğu gruptur.
<b>İlgili kullanıcı</b>	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 kişilerdir.
<b>İmha</b>	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir
<b>Kanun</b>	6698 Sayılı Kişisel Verilerin Korunması Kanunu'dur
<b>Kayıt ortamı</b>	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamdır
<b>Kişisel veri işleme envanteri</b>	Şirketin 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 oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı envanterdir
<b>Kurul</b>	Kişisel Verileri Koruma Kurulu'dur
<b>Periyodik imha</b>	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda işbu Politika'da belirtilen belirli zaman aralıklarında Şirket tarafından resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir
<b>Sicil</b>	30.12.2017 tarih 30286 Sayılı resmi gazete ile yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğe göre -Kurul tarafından tutulacak Veri Sorumluları Sicilidir.
<b>Veri kayıt sistemi</b>	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.
<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
<b>Yönetmelik</b>	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik'tir

## C. AMAÇ VE KAPSAM

İşbu Politika, Kanununun 7.maddesi uyarınca oluşturulan Yönetmelik içerisinde yer alan kişisel verilerin imhasından sorumlu olan gerçek veya tüzel kişiler hakkında uygulanır ve Şirket ile Şirket'in sözleşmesel olarak sorumlu olduğu üçüncü kişiler tarafından uyulması gereken esasları belirler.

Yönetmelik uyarınca Şirket, Sicile kayıt yükümlülüğü olan bir Veri Sorumlusu olarak, uhdesinde bulunan kişisel verileri kişisel veri envanterine uygun bir şekilde saklamak ve gerektiğinde imha etmek için işbu Politika'yı hazırlamak ve uygun hareket etmek ile yükümlüdür.

Kişisel verilerin saklanması ve imhasında aşağıdaki ilkeler geçerli olacaktır:

- a) Kanunun 4 üncü maddesindeki genel ilkelere uyulacaktır.
- b) Şirket, işbu Politikayı hazırlamış olmanın tek başına kişisel verilerin Yönetmelik, Kanun ve ilgili mevzuata uygun olarak imha edildiği anlamına gelmeyeceğini kabul etmektedir.
- c) Şirket, kişisel verileri saklarken yahut silerken, yok ederken veya anonim hale getirirken, Kanun'un 12. Maddesinde yer alan güvenlik tedbirlerine, ilgili mevzuatta yer alan hükümlere, Kurulu' un alacağı kararlara ve Politika'ya uygun hareket edeceğini kabul, beyan ve taahhüt eder.
- d) Şirket, bünyesinde bulundurduğu kişisel verilerin amacı tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin imhası sırasında işbu Politika'ya ve Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.
- e) Şirket, Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır. Söz konusu teknik ve idari tedbirler, kişisel verilerin saklanması ve imhası için kullanılacak yöntemlerle ilgili oluşturulan teknik kılavuzlarda tariflenir.
- f) Şirket, Kişisel verileri saklama ve imha süreçlerinde yer alacakların unvan, birim ve görev tanımlarını belirler.

#### **D. KAYIT ORTAMLARI**

Şirket, işbu Politika ile kişisel veri içeren ve aşağıda sayılmış olan ortamlar ve bunlara ek olarak ortaya çıkabilecek diğer ortamlardaki kişisel verileri Politika'nın kapsamına dâhil etmeyi kabul eder.

- a) Şirket adına kullanılan bilgisayarlar/sunucular
- b) Ağ cihazları,
- c) Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri,
- d) Mobil telefonlar ve içerisindeki tüm saklama alanları,
- e) Kâğıt,
- f) Mikrofiş,
- g) Yazıcı, Parmak izi okuyucu gibi çevre birimler,
- h) Manyetik bantlar,
- i) Optik diskler,
- j) Flash hafızalar.

#### **E. KİŞİSEL VERİLERİN İMHASINI GEREKTİREN DURUMLAR**

Aşağıda belirtilen kapsamda bir ihlal olması durumunda Potansiyel Güvenlik İhlal durumu kabul edilerek Şirket tarafından ilgili güvenlik ihlal süreçleri işletilecek bunlara ilişkin rapor ve bildirimler gerekli görülen durumlarda Şirket yönetimi, Kurul ve ilgili kişisel veri sahipleri nezdinde paylaşılacaktır. Bu amaçla söz konusu rapor ve bildirimlerin yapılması için Şirketin ihlal yönetimi süreçleri uygulanacaktır.

##### **1. Kanuna Aykırılık**

Şirket, kişisel verileri Kanunda belirtildiği şekle aykırı olarak işlemeyeceğini taahhüt eder.

Şirket, Kanunun 5 ve 6. maddelerindeki kişisel verilerin işlenmesi şartlarındaki istisnalar mevcut olmadığı sürece;

- a) Kanunda belirtilen istisnalar dışında açık rızasını almadığı kişilerin kişisel verilerini saklamayacaktır.
- b) İstisna kapsamında veya açık rıza kapsamında işlenen verilerin işleme amacının ortadan kalkması ve/veya yasal saklama sürelerinin dolması halinde Şirket bu kişisel verileri saklamayacak ve imha edecektir.

## 2. Kişisel Veri İşleme Şartlarının Ortadan Kalkması

Şirket, veri işleme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu kişisel veri işleyen ilgili tüm çalışanları ile paylaşır.

Çalışanlar, veri işleme şartlarının ortadan kalktığı durumlarda veri işlemeye devam etmeyecektir. Bu durumların tespiti ilgili iş biriminin önerisi ile Hukuk Müşavirliği tarafından yapılacaktır ve işbu Politika'ya uygun şekilde imha işlemi gerçekleştirir.

Şirket aşağıda listelenen ve Yönetmelik içinde de belirtilen ilgili durumlarda veri işleme şartlarının ortadan kalktığını kabul eder:

- İlgili mevzuatın kişisel verileri işlemeye esas teşkil eden hükümlerinin değiştirilmesi veya yürürlükten kaldırılması;
- Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçersiz olması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanununun 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı usule uygun başvurunun Şirket tarafından kabulü,
- Şirket, ilgili kişi tarafından kişisel verilerinin imhası talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami süre geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

## F. KİŞİSEL VERİLERİN İMHASI

Kişisel verilerin imhası, aşağıda detaylıca açıklanan verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde üç farklı şekilde yapılabilir.

Şirket bünyesinde ilgili iş birimleri, söz konusu kişisel verilerin bulunduğu bilgi sistemleri ve uygulama sahipleri, Hukuk Müşavirliği ve konuyla ilgili olabilecek diğer kişi ya da bölümler kişisel verilerin imhası için uygulanacak yöntem bu imhanın nedenine bağlı olarak yazılı karar verir. Bu yazılı karar gereğince işbu Politika'nın G maddesindeki imha yöntemlerinden biri Kurul'un yayınladığı Kişisel Verilerin Silinmesi Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi'ne bağlı olarak uygulanır.

Kişisel verilerin saklanması ve imhası için kullanılacak yöntemlerle ilgili Şirket ayrıca teknik kılavuzlar oluşturur ve bunların uygulanmasını sağlar.

Kişisel verilerin imhasının takibi Şirket içerisindeki ilgili veri sahibi iş biriminin sorumluluğundadır. Veri sahibi iş birimi, verilerin imhası için denetimi kendisi tarafından yapılmak kaydıyla Şirket'in farklı birimlerinden destek alır.

### 1. Kişisel Verilerin Silinmesi

Tamamen veya kısmen otomatik yollarla işlenen kişisel verilerin silinmesi; söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Herhangi bir veri kayıt sisteminin parçasını teşkil eden ve otomatik olmayan yollarla işlenen kişisel verilerin silinmesi sürecinde, yasal saklama süreleri göz önünde bulundurularak silme işlemine konu olacak kişisel veriler belirlenir. Şirket kişisel verilere erişim ve yetkilendirme anlamında Şirket'in mevcut durumda bilgi sistemleri ve uygulamaları üzerinde yürütmekte olduğu rol ve yetki matrisleri dâhilinde güncellemelerini yapar ve ilgili kullanıcıları tespit eder. İlgili Kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkileri ve yöntemleri bu kapsamda tespit edilir.

Şirket, kişisel verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirir. Şirket, bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti eder.

## 2. Kişisel Verilerin Yok Edilmesi

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

Yok etme işlemi, Şirket'in verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve Şirket bu verileri tekrar geri getirilmesi mümkün olmayacak hale getirmekle yükümlüdür.

Kağıt ve mikrofiş ortamları için bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makineleri ile anlaşılmaz boyutta geri birleştirilemeyecek şekilde küçük parçalara bölünerek yok edilecektir. Ayrıca, Şirket bu kapsamda Üçüncü Tarafardan imha hizmeti alabilir.

## 3. Kişisel Verilerin Anonimleştirilmesi

Anonim hale getirme işlemi, Şirket'in kişisel verileri tamamen veya kısmen otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Şirket, ilgili veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıları çıkartarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engelleyerek bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesini sağlar.

Verilerin anonimleştirilmesi sırasında Şirket, tek yönlü fonksiyonlar ile şifreleme gibi yöntemler kullanabilir.

## G. KİŞİSEL VERİLERİN İMHA YÖNTEMLERİ VE SÜRECİ

Kişisel verilerin imhası için Şirket, imha sırasında kullanılacak tüm yöntemleri İşbu Politika ve eklerinde tanımlar. Veri sahibi iş birimi, İşbu Politika içerisindeki uygun yöntemi uygun duruma göre belirleyerek uygulamakla yükümlüdür.

Kişisel verilerin imhası sırasında Şirket vereceği yazılı karara göre aşağıdaki yöntemlerden uygun olanı seçerek imhayı gerçekleştirir:

### 1. Üzerine Yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine yazılımlarla en az 7 kez 0 ve 1'lerden oluşan rassal veriler yazılarak eski verinin okunamaz hale getirilmesi işlemidir.

### 2. Manyetize Etme

Manyetik medyanın yüksek değerde manyetik alanda fiziksel değişime sokularak üzerindeki verinin okunamaz hale getirilmesi işlemidir.

### 3. Fiziksel Yok Etme

Optik medya veya manyetik medyanın eritme, toz haline getirme, öğütme ve benzeri işlemlerle fiziksel olarak yok edilmesi işlemidir. Manyetize etme veya üzerine yazma metodlarının başarısız olduğu durumlarda uygulanabilir.

### 4. Bulut İmhası

Bulut sistemler üzerinde tutulan kişisel verilerin imha bildirimini anlaşılabilir servis sağlayıcıya yapılmasının ardından kişisel verilerin şifreleme anahtarlarının tüm kopyalarının imha edilmesi işlemidir.

### 5. Çevresel Sistemlerde Yer Alan Kişisel Verilerin İmhası

Yazıcı, parmak izi ünitesi, kapı giriş turnikesi gibi sistemler içerisinde yer alan kişisel verileri barındıran mevcut ise iç ünite, mevcut değil ise tüm cihaz üzerinde üzerine yazma, manyetize etme veya fiziksel yok etme uygulanarak yapılması gereken imha işlemidir. Bu tip imhaların, cihazların yedekleme, bakım ve benzeri işlemlere tabi olmasından önce uygulanması zorunludur.

## H. SAKLAMA VE İMHA SÜRELERİ

### 1. Periyodik İmha ve Yasal Saklama Süreleri

Yasal saklama ve imha sürelerini dolduran fiziksel ve elektronik veriler, periyodik olarak imha edilir. Şirket, imha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işlemi, kişisel verileri imha eder.

Periyodik imha, tüm kişisel veriler için 6 aylık zaman aralıklarında gerçekleştirilir. Periyodik imha sırasında baz alınacak yasal saklama süreleri, Şirketin Kişisel Veri Envanteri'nde belirlenmiştir. İmha işlemi, imha yükümlülüğünün doğmasını takiben ilk Periyodik imha sırasında uygulanır.

İmha edilen kişisel verilere ilişkin tüm işlemler kayıt altına alınır ve bu kayıtlar 3 yıl süre ile saklanır.

## 2. Veri Sahiplerinin Talep Etmesi Durumunda İmha Süreci

Veri sahiplerinin Şirket'e başvurarak kendisine ait kişisel verilerin imhasını talep ettiği durumlarda, kişisel verileri işleme şartlarının mevcut durumunu kontrol eder. Söz konusu kontrol sonucunda;

- Kişisel verileri işleme şartlarının tamamının ortadan kalktığı anlaşılırsa, talebe konu kişisel veriler işbu Politika'da belirtilen karar ve yöntemlere uygun olarak en geç otuz gün içinde imha edilir ve ilgili kişiye bilgi verilir.
- Kişisel verileri işleme şartlarının ortadan kalktığı ve talebe konu olan kişisel verilerin üçüncü kişilere aktarıldığı anlaşılırsa Şirket bu durumu ilgili üçüncü kişiye bildirir; üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Şirket ilgili veri sahibine gerekçesini açıklayarak talebi reddedebilir ve ret cevabını ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

Veri sahiplerinden gelecek taleplerin karşılanması ve yanıtlanması amacıyla Şirket bünyesinde Kişisel Veri Sahiplerinden Gelen Talep ve Şikayetlerin Yönetimi Süreci oluşturulur.

## İ. SAKLAMA VE İMHA SÜREÇLERİNDE YETKİLENDİRME

Şirket, kişisel verileri saklama ve imha süreçlerinde görev alanlar ve iş tanımları aşağıdaki gibidir;

- KVKK Çalışma Grubu: Kişisel verilerin saklanması ve imhası konusunda Şirketin ilgili iş birimleri ile beraber çalışarak politika ve yöntemler hakkında karar verir, Politika ve eklerinin güncel tutulmasına sağlar, gerekli durumlarda Şirketin Süreç Yönetimi, Bilişim ve diğer birimlerle yakın çalışarak Politika'nın Kanun ve Yönetmeliğe uygun ve doğru şekilde yürütülmesini temin eder.
- Hukuk Müşavirliği: Kişisel verilerin saklanması ve imhası ile ilgili hukuki konularda danışmanlık yapar, Kanun, Yönetmelik ve ilgili mevzuat değişikliği halinde ilgili iş birimlerine gerekli bilgilendirmeyi yapar. Politika'nın Kanun ve Yönetmeliğe uygun olarak yürütülmesini temin eder.
- Bilgi teknolojileri: Politika'da belirtilen karar ve yöntemler ışığında ilgili imha ve saklama süreçlerinin Kanun ve Yönetmeliğe uygun şekilde gerçekleştirilmesini sağlar.
- Şirket'in ilgili iş birimleri: Kişisel verilerin saklanması ve imhası konusunda politika ve yöntemlerin belirlenmesi için görüş ve gerekçelerini belirtir ve bu Politika nezdinde yürütülmesi aksiyonların takibini yapar.

## J. POLİTİKA'DA YAPILACAK DEĞİŞİKLİKLER

1. Kanun, Yönetmelik veya sair mevzuatın kısmen veya tamamen değiştirilmesi, tadil edilmesi, güncellenmesi veya yürürlükten kaldırılması durumunda, Şirket Politikayı yeni Kanun, Yönetmelik veya mevzuata uyumlu olacak şekilde güncelleyerek değiştirecektir.
2. Şirket, Politika üzerinde yaptığı değişiklikler incelenebilecek olacak şekilde güncellenen Politika'yı e-posta yolu ile çalışanlarıyla paylaşacak ve kurumsal intranet üzerinden çalışanlarının erişimine sunacaktır.



#### **K. POLİTİKA'NIN YÜRÜRLÜK TARİHİ**

İşbu Politika **26.05.2021** tarihinde yürürlüğe girmiştir.