

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Kapsamında kişisel verisini işlediğimiz veri sahiplerinin verilerinin ne kadar süre sitemimizde tutulduğunu ve imha koşulları, süreleri hakkında bilgilendirmek isteriz. Veri sorumlusu ECETAŞ İNŞAAT SAN. VE TİC. A.Ş ve işletmesi Ecesaray Marina&Resort sözkonusu imha politikası uygulanacaktır.

Tanımlar

Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

Veri İşleyen: 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.

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

VERBİS: Veri Sorumluları Sicil Bilgi Sistemi.

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.

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.

Yönetmelik: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

Politika: Kişisel Verileri Saklama ve İmha Politikası

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

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.

Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.

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 ve tekrar kullanılamaz hale getirilmesi işlemi.

Kurul: Kişisel Verileri Koruma Kurulu.

Periyodik İmha: Kanun'da 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.

Veri Sahibi/İlgili Kişi: Kişisel verisi işlenen gerçek kişi.

Kişisel Veri Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek

oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandıkları envanter.

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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Periyodik İmha : Kanunda 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.

İlkeler

Öncelikle şirket olarak gereklere uygun bir veri saklama yöntemi ve aracı kullandığımızı belirtmek isteriz.

* 6698 sayılı yasaya ve yönetmeliklere ve 108+ sözleşmesine ve Kişisel Verilerin Korunması Kurulu Kararların aykırı bir imha politikası benimsenmemelidir.

*Öncelikli olarak yetkisiz erişim, değiştirme veya yayımlama yanında kazara veya yetkisiz tahribe karşı otomatik veri dosyalarında yer alan kişisel verilerin korunması için uygun güvenlik önlemleri alınmıştır.

*Hem kazara kayıp veya tahrip gibi doğal tehlikelere karşı, hem de yetkisiz erişim, verilerin dolandırıcılık amacıyla kötüye kullanımı gibi insan kaynaklı tehlikelere ya da bilgisayar virüslerinin bulaşmasına karşı dosyaları koruyacak uygun önlemler alınmıştır.

*Kişisel verilerin korunması politikamız ve aydınlatma metninde belirttiğimiz alanlarda topladığımız kişisel verileriniz güvenli alanda kayıt altına alınmakta, saklanmakta ve hukuki yükümlülükler gereği saklama faaliyetimiz hariç en az 3 yıl saklanmaktadır.

*6698 sayılı Kanun ve Yönetmelik tarafımıza kişisel verilerin imha yöntemi sürecini seçme ve yönetme hakkı tanımıştır. Kişisel verinin türüne göre veri sorumlusu imha yöntemini kendisi belirleyecektir. İlgili kişinin talebi olması durumunda ise uygun yöntem gerekçe açıklayarak seçilecektir. Veri sorumlusu veriyi imha etmeden önce ilgili kişinin kayıtlı e-posta adresine ya da kayıtlı adresine bildirim yapacak ve verinin hangi yöntemle imha edileceği bilgisini verecektir.

*Kişisel veriler imha edilirken de bu süreçte gerekli idari ve teknik tedbirler alınacaktır. İmha edildikten sonra kayıt altına alınacak ve güvenli bir ortamda en az 3 yıl saklanacaktır. Hukuki yükümlülükler dolayısı ile tutulacak süre hükümleri saklıdır.

*Şirketimizde aktif olmayan müşteri, çalışan aday, çalışan, taşeron ve tedarikçi verileri kanunda tutulma süreleri hariç olmak üzere derhal imha edilecek ve imha edildiğine dair bilgi ile imha yöntemi ilgili kişiye uygun yöntemle bildirilecektir.

* Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından resen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.

*İlgili kişi de şirketten verilerinin silinmesini talep edebilecektir. Bu durumda şirket en geç 30 gün içerisinde başvuruya yanıt verir ve verilerin aktarıldığı gruplar da başvuru hakkında bilgilendirilecek ve silme şartları oluştu ise veri silinecektir. Silinme şartları oluşmayan kişisel verilerin neden dilinmediği ile ilgili gerekçeli olarak ilgili kişiye yanıt verilecek ve ne zaman silineceği bilgisi de verilecektir.

Saklama ve İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

İlgili kişinin kişisel verileri,

- ✓ Rezervasyon, ulaşım, ödeme, yerleşim süreçlerini yönetmek, tamamlamak,
- ✓ İletişim kurabilmek,
- ✓ Ürünlerimiz, kampanyalarımız, promosyonlarla ilgili bilgi vermek,
- ✓ Hizmetlerin özelleştirilerek sizlere sunmak,
- ✓ Analiz yapmak,
- ✓ Şirketimiz ve şirketimizle iş ilişkisi içinde bulunan kişilerin hukuki ve ticari güvenliğini sağlamak,
- ✓ İdari operasyonlar düzenlemek,
- ✓ Şirkete ait bölümlerin fiziksel güvenliğini ve denetimini sağlamak,
- ✓ İş ortağı/müşteri/tedarikçi değerlendirme süreçlerinde kullanmak,
- ✓ Şirketimizin ticari iş stratejilerini belirlemek ve uygulamak,
- ✓ Şirketimizin insan kaynakları politikasının yürütülmesini temin etmek,
- ✓ İlgili mevzuatlarla belirlenen yasal yükümlülükleri yerine getirmek ve bilgi vermek
- ✓ Marinanın yönetimini ve güvenliğini sağlamak,
- ✓ Tekne bağlama sözleşme ilişkisini kurmak ve sözleşme ilişkilerinin devamını sağlamak,

Amacıyla;

Konaklama hizmeti için,

- Kimlik bilgileri:(Adı-soyadı, doğum yeri ve tarihi, uyruk, T.C Kimlik numarası, pasaport numarası, Beraberindeki misafir adı-soyadı, doğum yeri ve tarihi)
- İletişim Bilgisi : (Adres, telefon numarası, e-posta)
- Finansal bilgiler : (Sadece Banka hesap numarası, Kredi kartı bilgileri)
- Araç Plaka Bilgisi:(Giriş-çıkış kayıt)

Marina hizmeti için,

- Kimlik Bilgileri
- İletişim Bilgileri (Adres, telefon numarası, e-posta,)
- Mülkiyet Bilgileri (Tekne mülkiyeti)(Tekne bağlama kütüğü ruhsatnamesi, Transitlog)
- Mürettebat bilgileri ve Belgeleri (Yetki belgesi, Sgk bilgileri, yeterlilik belgesi)
- Tekne Sahibi Araç Plaka No (Otopark kullanımı için)
- Tekne Sigorta Bilgisi
- Finansal Bilgiler (Sadece Banka hesap numarası, Kredi kartı bilgileri)

Kişisel verileriniz kayıt altına alınmaktadır. Yukarıda tanımlanmış verileriniz sözleşme ilişkisi çerçevesinde tarafınızdan istenmekte ve işlenmektedir.

Bu nedenlerle;

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

Hususlarına dikkat edilmektedir.

Verileriniz ;

- *Kişisel verilerinizin saklama süresi doldu ise ya da mevzuattan dolayı saklama koşullarında değişiklik nedeni ile zorunluluk ortadan kalktı ise,
- * Kişisel verilerin işleme amacının ortadan kalkması,
- * Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- *İlgili kişinin açık rızası ile işlenen kişisel verilerde ilgili kişinin açık rızasını geri alması,
- *İlgili kişinin KVKK m.11 kapsamında yaptığı başvurunun kabulü,
- *Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve Kurul tavsiyesi ile,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması halinde silinir ve imha edilir.

Saklama ve İmha Süreleri

Saklama ve imha süreleri belirlenirken Şirket 6698 sayılı yasa ve Yönetmelik kapsamında aşağıda yer alan kriterleri değerlendirir:

- *İlgili sektörde genel teamül gereği kabul edilen süre,
- *İşlemeyi gerekli kılan ve ilgili kişi ile tesis edilen hukuki ilişkinin devam edeceği süre,
- *Veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
- *Saklamanın yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- *Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
- *Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
- *Kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi.

Saklama süresi ortadan kalkan kişisel veriler, imha süreleri göz önünde bulundurularak 6 aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak anonim hale getirilir veya

imha edilir. Kişisel verilerin silinmesi, yok edilmesi ve 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.

Kişisel Verilerin Saklanması ve İmhasına İlişkin Teknik ve İdari Tedbirler

İdari Tedbirler:

Şirket idari tedbirler kapsamında;

- 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 kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- Kişisel verilerin bulunduğu ortama göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmasını sağlar ve bu ortamlara yetkisiz giriş çıkışları engeller.

Teknik Tedbirler:

Şirket idari tedbirler kapsamında;

Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır. Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler önlemler alınmaktadır.

*Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal(sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

*Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

*Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.

*Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır. Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

*Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.

*Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

* Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

*Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır. Kişisel verilerin güvenli olarak saklanması sağlayan veri yedekleme programları kullanılmaktadır.

*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. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

Kişisel Verileri Koruma Birimi'nin Görev ve Yetkileri

Kişisel Verileri Koruma Birimi, Kişisel Verilerin Korunması ile ilgili Politika ve diğer bilgilendirmeleri birimlere duyurur ve birimlerin bu konuda gelişimlerini takip eder. Periyodik olarak eğitim süreçlerini planlar ve denetimleri yaptırır. Konu ile ilgili mevzuat değişikliklerini takip eder ve Politika ve metinlerin mevzuata göre güncellenmesini sağlar. Kurul kararlarını düzenli olarak takip eder.

Politikanın Yürürlüğe Sokulması, İhlal Durumları ve Yaptırımlar

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

*Politikaya aykırı hareket edenler olduğunda ilgili birim amiri doğrudan veri sorumlusunu ve veri sorumlusunun atadığı irtibat kişisini bilgilendirir ve politikanın uygulanmasını sağlamak üzere gerekli tedbirleri alır.

*Politikaya aykırı davranış hakkında Kişisel Verileri Koruma Birimi de bilgilendirilir.

*Politikaya aykırı davranışlar hakkında gerekli işlem kısa zamanda yapılır.

EK-1 Personel Unvan,Birim ve Görev Listesi

EK-2 Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo

Kişisel veriler politika'nın 4. maddesinde belirtilen hususlar dikkate alınarak aşağıdaki tabloda belirtilen süreler boyunca saklanarak, süre sonunda ise anonim hale getirilecek veya yok edilecektir :

Süreç	Saklama Süresi	İmha Süresi
İş Kanunu kapsamında saklanılan veriler (örn. performans kayıtları vs.)	İş ilişkisinin sona ermesine müteakip 5 yıl	Saklama süresinin bitimini takiben 6 ay içerisinde
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (sağlık raporları vs.)	İş ilişkisinin sona ermesine müteakip 15 yıl	Saklama süresinin bitimini takiben 6 ay içerisinde
SGK mevzuatı kapsamında tutulan veriler	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 6 ay içerisinde
İş kazası/meslek hastalığına ilişkin bir talepte/davada kullanılabilecek dökümanlar	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 6 ay içerisinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takiben 6 ay içerisinde
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması	Dava zaman aşımı müddetince	Saklama süresinin bitimini takiben 6 ay içerisinde
Müşteri verileri	Kayıt altına alınmasına müteakip 10 yıl	Saklama süresinin bitimini takiben 6 ay içerisinde

Yukarıda düzenlenen sürelerden daha uzun süre saklanması gereken veriler ile ilgili Şirket haklarını saklı tutar ve ilgili kişinin talebi halinde gerekçesi ile birlikte silinme koşullarını açıklar.