GENEL İNŞAAT LİMİTED ŞİRKETİ

KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

OCAK 2021

İÇİNDEKİLER

1. İMHA POLİTİKASININ NİTELİĞİ VE AMACI

1.1. Giriş

İşbu imha politikası **Genel İnşaat Limited Şirketi** ("GenelİnŞ.") olarak elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin **"GenelİnŞ"** tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, "GenelİnŞ." nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri "Genel İnşaat Kişisel Verilerin İşlenmesi ve Korunması Politikası" ve işbu "Kişisel Veri Saklama ve İmha Politikası" çerçevesinde kanunlara uygun olarak yönetilmektedir.

1.2. Tanımlar Ve Kısaltmalar

TANIMLAR	**AÇIKLAMALAR** *Tablo 1 : Tanımlar*
Politika	"GenelİnŞ" elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı ifade eder.
İmha Politikası	"GenelİnŞ." elinde bulunan kişisel verilerin saklanması ve imha edilmesine ilişkin usul ve esasları belirleyen politikayı ifade eder.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Çerez (Cookie)	Kullanıcıların bilgisayarlarına yahut mobil cihazlarına kaydedilen ve ziyaret ettikleri web sayfalarındaki tercihleri ve diğer bilgileri depolamaya yardımcı olan küçük dosyalardır.
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 kişilerdir.
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 Sicile kayıt esnasında bildirilen gerçek kişi. (İrtibat kişisi Veri Sorumlusunu temsile yetkili değildir. Adından anlaşılacağı üzere yalnızca veri sorumlusu ile ilgili kişilerin ve Kurumun iletişimini "irtibatı" sağlamak üzere görevlendirilen kişidir.)
Kişisel Veri Kategorileri	"Politika" Tablo 3'de yer alan Kişisel Verilerin Genel İnşaat Veri haritasına göre kategorize edilmiş veri kategorilerini ifade eder.
Kişisel Veri Sahibi Kategorileri	"Politika" Tablo 4'de yer alan Kişisel Verilerin Sahiplerinin Genel İnşaat Veri haritasına göre kategorize edilmiş veri sahipleri kategorilerini ifade eder.
Paylaşılan Taraflar	"Politika" Tablo 5'de yer alan Kişisel Verilerin Paylaşıldığı kişileri Genel İnşaat Veri haritasına göre kategorize edilmiş kişisel veri paylaşım taraflarını ifade eder.
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	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 **İlgili Kullanıcılar** için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi. *Bkz: İlgili Kullanıcı Tanımı
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
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.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Veri İhlalleri	Kişisel verilerin kanuna aykırı şekilde ele geçirilmesi, toplanması, değiştirilmesi, kopyalanması, dağıtılması veya kullanılmasına dair haklı şüphelerin olduğu olaylardır.
KVK Birimi	"GenelİnŞ" bünyesinde kurulan kişisel verilerin korunması mevzuatı ve Genel İnşaat "Politikası" na uygun olarak kişisel verilerin işlenmesine yönelik süreçleri yönetmekle, gerekli idari ve teknik tedbirlerin alınmasını temin etmekle görevli birimdir.
Kaynak:	6698 sayılı Kişisel Verilerin Korunması Kanunu- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik - Veri Sorumluları Sicili Hakkında Yönetmelik - Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ - Veri Sorumlusuna Başvuru ve Usul Esasları Hakkında Tebliğ Veri sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

2. SORUMLULUK VE GÖREV DAĞILIMI

2.1. Kişisel Verileri Koruma Birimi

"GenelİnŞ." tarafından, Kişisel Verilerin Korunması hakkında mevzuata, idari kararlara, yargı kararlarına ve "GenelİnŞ." Politikalarına ve iç düzenlemelerine uygun hareket edilmesi amacıyla, Kişisel Verileri Koruma Birimi kurulmuş olup, "GenelİnŞ." ın tüm birimleri ve çalışanları, "Politika" kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesinin ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında "GenelİnŞ." Yönetim Kuruluna ve diğer sorumlu birimlere aktif olarak destek verir.

Kişisel Verileri Koruma Birimi, "GenelİnŞ." Politikalarının hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi, ilgili birimlere verilecek eğitimlerin belirlenmesi, çalışanların bilinçlendirilmesi, gerekli idari ve teknik tedbirlerin alınması, Veri İşleme Sözleşmesi ve Gizlilik Sözleşmelerinin hazırlanması ve nihai hale getirilmesi, dokümantasyon setinde kişisel verilerin korunması amacıyla hazırlanacak ek dokümanların belirlenmesi ve "GenelİnŞ." bünyesinde kişisel verilere erişimi olan kişilerin politikaya uygun hareket etmesinden yönetim kuruluna karşı sorumludur.

"GenelİnŞ." tarafından imzalanacak metinlerde Gizlilik ve/veya KVK maddesi yer alması gerekip gerekmediği hakkında görüşlerini bildirir ve gerekli olması halinde gerekli dokümantasyonu hazırlar ve KVK Birimi Başkanı nihai onayı ile "GenelİnŞ." imzaya yetkili kişiye ibraz edilir.

Kişisel Verileri Koruma Birimi 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 ve 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. Politika, Birim Başkanı'nın önderliğinde, Birim üyeleri tarafından takip edilir, yürütümü sağlanır ve güncellenir.

2.2 Veri İşleyenlerin Sorumluluğu

Kişisel verilerin "GenelİnŞ." adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, veri sorumlusu olarak "GenelİnŞ." ile veri işleyen kişiler, veri güvenliğine yönelik tedbirlerin alınması konusunda idari makamlara ve ilgili kişilere karşı Kanunen müştereken sorumlu olurlar. Bu minvalde, Veri işleyenler asgari olarak "GenelİnŞ." in almış olduğu tedbirleri almakla ve iş burada belirtilen imha sürelerine ve yöntemlerine ve "GenelİnŞ." Kişisel Verilerin İşlenmesi ve Korunması Politikası'na ve diğer "GenelİnŞ." Politikalarına uymakla sorumludur. "GenelİnŞ.", veri sorumlusu olarak, kendisi ile kişisel verilerini paylaşan ilgili kişilere sağladıkları güvenin; iş ortakları, tedarikçi ve yüklenicileri tarafından da aynı şekilde sürdürülmesinin sağlanması için periyodik olarak, veri işleyenlerin Kişisel Verilerin Korunması mevzuatına ve idari kararlar ile Yargı kararlarına uyumunu denetler.

"GenelİnŞ." bünyesinde yer alan Kişisel Verileri Koruma Birimi, veri işleyenlerin sorumluluklarına ilişkin tedbirlerin alınması, sözleşmelerin imzalanması amacıyla gerekli tedbir ve önlemleri alır.

2.3 Saklama ve İmha Politikasının Yürürlüğe Sokulması

İmha Politikası, "GenelİnŞ." Şirket merkezinde asılmasının ve/veya çalışanlara duyurulmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, İmha Politikası'nın ıslak imzalı eski nüshaları "GenelİnŞ." Yönetim Kurulu Kararı ile Kişisel Verileri Koruma Birimi tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır.

İmha Politikası, yürürlüğü itibariyle tüm iş birimleri, dış hizmet sağlayıcıları (danışmanlar, tedarikçiler, alt işverenler vb) ve kişisel veri işleyen herkes için bağlayıcı olacaktır. Çalışanların politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların müdürlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde konu ilgili çalışanın müdürü tarafından vakit kaybetmeksizin ve en geç 24 saat içinde Kişisel Verileri Koruma Birimi'ne bilgi verilecektir. Politikaya aykırı davranan çalışan hakkında, yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır.

2.4 Kişisel Verilerin Saklama Ve İmha Süreçlerinde Görev Alanların Unvanları, Birimleri Ve Görev Tanımları

Tablo 2: Saklama Ve İmha Süreçleri Görev Dağılımı

UNVAN	BİRİM	GÖREV
"GenelİnŞ." Yönetim Kurulu Üyeleri	Yönetim Kurulu	❖ "GenelİnŞ." KVK Birimi'nin kurulması, üyelerinin seçilmesi, görev tanımlarının belirlenmesi, KVK Biriminin etkin çalışması ve denetlenmesinden, ❖ Erişimi olan kişilerin politikalara uygun hareket etmesinden sorumludur.
Kişisel Veri Koruma Birimi Başkanı	Kişisel Verileri Koruma Birimi	❖ KVK Biriminin Başkanı olup, KVK Biriminin çalışmalarını koordine edecek, birimin etkin ve verimli çalışmasını temin edecek kişidir. ❖ Veri İşleme Sözleşmelerinin son onayının verilmesi, ❖ Gizlilik Sözleşmelerinin son onayının verilmesinden sorumludur.
Kişisel Veri Koruma Birimi Üyeleri	Kişisel Verileri Koruma Birimi	❖ Kişisel Verilerin İşlenmesi ve Korunmasına Yönelik Politikaların hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi, ❖ İlgili birimlere verilecek eğitimlerin belirlenmesi, çalışanların bilinçlendirilmesi, ❖ Gerekli idari ve teknik tedbirlerin alınması, ❖ Verilerin aktarılması ile ilgili süreçlerin yönetilmesi, ❖ Veri İşleme Sözleşmesi ve Gizlilik Sözleşmelerinin hazırlanması ve nihai hale getirilmesi, ❖ Dokümantasyon setinde kişisel verilerin korunması amacıyla hazırlanacak ek dokümanların belirlenmesi, ❖ "GenelİnŞ." bünyesinde kişisel verilere erişimi olan kişilerin politikaya uygun hareket etmesinden yönetim kuruluna karşı sorumludur. ❖ Birim bünyesinden seçilecek irtibat kişisi aracılığı ile Kurul ile iletişimin sağlanmasının temin edilmesinden, ❖ İlgili kişilere verilecek cevapların düzenlenmesinden ve sürecin yönetilmesinden, ❖ Başvuru ve Şikayet ve Yargı Süreçlerinin Yönetilmesi ve yürütülmesinden sorumludur.
İdari İşler Departmanı Müdürü	İdari İşler Departmanı	❖ Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
Finans Departmanı Müdürü	Finans Departmanı	❖ Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
Hukuk Departmanı	Hukuk ve Regülasyon Departmanı	❖ Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
İş Geliştirme ve Planlama Departmanı Müdürü	İş Geliştirme ve Planlama Departmanı	❖ Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
Veri Güvenliği ve Bilgi Sistemleri İş Ortağı	Veri Güvenliği ve Bilgi Sistemleri İş Ortağı	❖ Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve gerekli yatırımların sağlanması için yönetim kurulunun bilgilendirilmesinden, ❖ Elektronik kayıt ortamlarında

		❖ Gerçekleştirilen silme, yok etme, anonimleştirme işlemleri bakımından yürütüm ve iç denetimlerden sorumludur.
"GenelİnŞ." Bünyesindeki tüm çalışanlar	Çalışanlar	❖ Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

3. KAYIT ORTAMLARI VE GÜVENLİK TEDBİRLERİ

3.1. Kişisel Verilerin Saklandığı Ortamlar

"GenelİnŞ." 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. **"GenelİnŞ."** her halde veri sorumlusu sıfatıyla 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.

Tablo 3- Kişisel Verilerin Saklandığı Ortamlar

a) Matbu ortamlar	:	❖ Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır. ❖ Manuel veri kayıt sistemleri (katılımcı formları, toplantı tutanakları, katılımcı formları, çalışma tutanakları, İnsan Kaynakları form ve dilekçe örnekleri v.b) ❖ Yazılı, basılı, görsel ortamlar ❖ Birim Dolapları ❖ Arşiv alanları
b) Yerel dijital ortamlar	:	❖ **"GenelİnŞ."** bünyesinde yer alan sunucular (etki alanı, yedekleme, e-posta veri tabanı, web, dosya paylaşımı vb.) ❖ Yazılımlar (MS Office yazılımları, portal vb) ❖ Bilgi Güvenliği Cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb) ❖ Kişisel Bilgisayarlar (masaüstü, dizüstü) ❖ Mobil cihazlar(telefon, tablet) ❖ Kapalı Sistem Kamera Kayıt Ortamı ❖ Sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır. ❖ Yazıcı, tarayıcı, fotokopi makinesi
c) Bulut ortamlar	:	❖ **"GenelİnŞ."** bünyesinde yer alma**ma**kla birlikte, **"GenelİnŞ."**'in ileride kullanması halinde şifreli ve günvelik tedbirleri uygulanacak ortam.

3.2. Ortamların Güvenliğinin Sağlanması

"GenelİnŞ." , kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

3.2.1. Teknik Tedbirler

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

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.

3.2.2. İdari Tedbirler

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

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- 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.
- Mevcut risk ve tehditler belirlenmiştir.

3.2.3. Kurum İçi Denetim

"GenelİnŞ." , Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin kurum içi denetimler yapmaktadır.

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

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

4. SAKLAMA VE İMHA NEDENLERİ

"GenelİnŞ." tarafından; çalışanlar, çalışan adayları, şirket paysahipleri, yönetim kadrosu, "GenelİnŞ." çalışmalarına katılan kişiler, "GenelİnŞ." Faaliyetlerine bulunanlar, İnceleme ve Denetim faaliyetlerine dahil olanlar ve "Politika" da "Kişisel Veri Sahibi Kategorilerinde yer alan kişilerin ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin kişisel verileri Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1. Saklama Nedenleri

Kanunun 3 üncü maddesinde *kişisel verilerin işlenmesi* kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin *işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi* gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise *kişisel verilerin işleme şartları* sayılmıştır.
Buna göre, "GenelİnŞ." faaliyetleri çerçevesinde kişisel veriler, *ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.*

"GenelİnŞ." bünyesinde tutulan kişisel veriler Kanun ve "Politika" (ilgili politikaya "www.genelinsaat.com.tr" adresinden ulaşabilirsiniz) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

Saklamayı Gerektiren İşleme Amaçları

Kişisel veriler, "GenelİnŞ." tarafından özellikle;

(i) ticari faaliyetlerin sürdürülebilmesi,

(ii) hukuki yükümlülüklerin yerine getirilebilmesi,

(iii) çalışan haklarının ve yan haklarının planlanması ve ifası için Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

(iv) Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.

(v) İnceleme ve Denetleme faaliyetlerinin ifa edildiğinin ispatlanması, yürütülmesi, organize edilmesi

Ayrıca, "GenelİnŞ."in faaliyetleri çerçevesinde işlemekte olduğu kişisel verilere ilişkin saklama amaçları aşağıda detaylı şekilde belirtildiği şekildedir.

- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- İlgili kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından ilgili kişilerin açık rızasının bulunması.
- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak ve ilişkilerin yürütülmesini temin etmek,
- Şirket pay sahipleri ve pay sahipliği hakları, genel kurul, yönetim kurulu, inceleme ve denetleme işlemlerinin yürütülmesi,
- Şirket çalışanları ile ilişkilerin yürütülmesi,
- Finans ve Muhasebe işlemlerinin yürütülmesi,
- "GenelİnŞ." faaliyetlerinin ifası için toplantı, organizasyon, iş geliştirme, etkinlik, konferans ve benzeri etkinliklerin düzenlenmesini temin etmek,
- Ulusal ve uluslararası kurum ve kuruluşlarla kuruluş amacına yönelik konularda işbirliği yaparak sağlayacağı bilgi, belge ve dokümanlardan yararlanarak çalışmalar gerçekleştirmek,

belge ve yayınları tercüme etmek, ettirmek ve bu dokümanların yayımını yapmak, bilgi bankası oluşturmak,

- Çalışma Grupları ve Toplantı tutanaklarını arşivleyerek strateji belirlemek ve çalışma gruplarının etkin çalışmasını koordine etmek,
- Hukuki, Adli Süreçleri Takip Etmek, ispat vasıtası delil ve belgeleri arşivlemek, yükümlülükleri ifa etmek, gerektiğinde cevap, yazışmaların tevsik edici belgelerini arşivlemek
- İdari süreçleri takip etmek, ispat vasıtası delil ve belgeleri arşivlemek, yükümlülükleri ifa etmek, gerektiğinde cevap, yazışmaların tevsik edici belgelerini arşivlemek
- Talep, Şikayet, İtiraz, İhbar, İtiraz, İhtarname dahilinde ispat vasıtası delil ve belgeleri arşivlemek, yükümlülükleri ifa etmek, gerektiğinde cevap, yazışmaların tevsik edici belgelerini arşivlemek
- Sözleşmeler ve protokollerin ifası,
- Sosyal sorumluluk projeleri faaliyet kayıtlarının arşivlenmesi.
- Kişisel Verilerin Korunması Kanunu kapsamında ilgili kişilerin talep ve şikayetlerin sonuçlandırılması,
- Kişisel Verilerin Korunması Kanunu kapsamında gerekli teknik önlemlerin alınmasını temin etmek (veri yedekleme, silme yok etme işlemlerinin kayıt altına alınması, erişim log kayıtlarının tutulması vb.),
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- "GenelİnŞ." ile iş birliğinde bulunan gerçek/tüzel kişilerle irtibat sağlamak, yükümlülüklerin ifasını temin etmek,
- Fiziksel mekan ve çalışan güvenliğini temin etmek,
- İnceleme ve Denetleme Faaliyetlerinin gereği gibi yerine getirildiğinin ispatı, inceleme ve denetleme faaliyetlerinin yürütülmesi, belge güvenliğinin temini alt amaçları dahilinde fiziksel mekan güvenliğini temin etmek,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla "GenelİnŞ."in meşru menfaatleri için saklanmasının zorunlu olması,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü

4.2. Saklamayı Gerektiren Hukuki Sebepler

"GenelİnŞ." faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4721 sayılı Türk Medeni Kanunu,
- 4734 sayılı Kamu İhale Kanunu
- 213 sayılı Vergi Usul 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,
- 4857 sayılı İş Kanunu,
- 1136 sayılı Avukatlık Kanunu
- 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.3. İmha Nedenleri

"GenelİnŞ." bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun "GenelİnŞ." tarafından kabul edilmesi,
- "GenelİnŞ." in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi üzerine, verilen cevabı yetersiz bulması veya "GenelİnŞ."in öngörülen süre içinde cevap vermemesi hallerinde; ilgili kişinin Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, "GenelİnŞ." tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.4. İmha Yöntemleri

"GenelİnŞ." , Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

"GenelİnŞ." tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

4.4.1 Silme Yöntemleri

Matbu 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.
Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri		
Yazılımdan güvenli olarak silme	:	GenelİnŞ. Bünyesinde bulut sistemi kulanılmamakla beraber, ileride bulut sisteminin kullanılması halinde, bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

4.4.2 Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri		
Fiziksel yok etme	:	Matbu ortamda tutulan belgeler evrak tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri		
Fiziksel yok etme	:	Kişisel veri barındıran optik ve manyetik medyanın parçalanması ile fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı parçalama gibi işlemlerle verilerin erişilmez kılınması sağlanır.
De-manyetize etme (degauss)	:	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
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	:	GenelİnŞ. Bünyesinde bulut sistemi kulanılmamakla beraber, ileride bulut sisteminin kullanılması halinde, 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.

4.4.3. 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 bir kaçının 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.

"GenelİnŞ." , kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. **"GenelİnŞ."** , bu anonimleştirme yöntemlerini kullanırken K-Anonimlik [UN2] (K-Anonymity), L-Çeşitlilik (L-Diversity) [UN3] ve T-Yakınlık [UN4] (T-Closeness) istatistik yöntemlerini kullanabilir[1].

5. SAKLAMA VE İMHA SÜRELERİ

"GenelİnŞ."'in kişisel verileri saklama süresi ilgili mevzuatta belirlenen süreler dikkate alınarak hesaplanmaktadır. Bununla beraber, faaliyetlerin yürütülmesi amacıyla şirketin, bireylerle iletişim halinde olması şirket sözleşmesindeki amacı gerçekleştirmek bakımından önem taşımaktadır.

KVK Kanununda yer alan kişisel veri işleme şartlarının varlığını ortadan kaldıracak kişisel veri işleme amaçlarının sona ermesi halinde, "GenelİnŞ." tarafından kişisel veriler imha edilecektir. Söz konusu imha işlemleri ilgili mevzuatın hükümlerine uygun olarak **6 aylık periyotlarla** re'sen gerçekleştirilmekte ya da veri sahiplerinden gelen taleplerin gerektirmesi halinde neticeye bağlanmaktadır. İlaveten, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11/3 maddesi gereğince, kişisel verileri imha yükümlülüğünün ortaya çıktığı tarihi takip eden **3 ay** içinde kişisel veriler "veri kategorisi durumuna göre silinecek, anonim hale getirilecek ve/veya yok edilecektir. Yönetmeliğin 12. maddesi gereğince ise, ilgili kişinin silme ve/veya yok etme taleplerini "GenelİnŞ." mevzuatta başkaca bir süre öngörülmediği takdirde en geç **30 gün** içinde yerine getirerek ilgili kişiye bilgi verecektir.

Kişisel Verilerin imhası ile ilgili tutanaklar ise "GenelİnŞ." tarafından mevzuat gereğince başkaca bir süre belirlenmediği takdirde **3 yıl** süre ile saklanacaktır.

"GenelİnŞ." tarafından kişisel verilerin imhası, kişisel verilerin yer aldığı ortamlara göre silme, anonimleştirme ya da yok etme teknikleri kullanılarak yerine getirilmektedir. Söz konusu teknikler hakkında detaylı bilgiler Kurul tarafından yayınlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi içerisinde yer almaktadır.

Kişisel verilerin **ilgili kullanıcılar için** hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemine kişisel verinin **silinmesi denir**. İlgili Kullanıcı tabiri ise, verilerin teknik olarak depolanması,

[1] [UN1]-Kullanılan diğer ortamlar var ise bunların belirlenmesi, burada belirtilen ve ancak kullanılmayan bir ortam var ise buradan çıkarılması gerekmektedir.
[UN2]-Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.
[UN3]-Anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.
[UN4]-Çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

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.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7/5. maddesi gereğince veri işleme sebeplerinin ortadan kalkması halinde ve/veya ilgili kişinin talebi üzerine (Eğer ki KVKK Kanunu m. 5/2 ve 6/3 dahilinde yer alan açık rıza alınmasına gerek olmayacak şekilde veya KVK Kanunu m. 28 dahilinde kanuni istisna kapsamına girmiyorsa) "GenelİnŞ." bünyesinde oluşturulan "KVK Birimi" tarafından kişisel veriler **ilgili kullanıcılar için** hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek şekilde **silinecektir.**

İlgili Kişiler bakımından önemle belirtmek isteriz ki, KVK Kanunun 5/2 ve 6/3 kişisel verilerin "ilgili kişilerin" açık rızası alınmadan işlenme şartları ve KVK Kanunu m. 28 hükmünde Kanun hükümlerinden istisna halleri belirtilmiştir. Söz konusu işlenme şartlarının devam etmesi halinde ilgili kişiden "açık rıza" dahi alınmış olsa, ilgili kişi açık rızasını kaldırmak suretiyle verilerin imhasını ve veri işlenmesine son verilmesini talep etse dahi, talebinin reddi söz konusu olabilecektir.

Tablo 4 : Süreç Bazında Saklama Ve İmha Süreleri Tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Genel Kurul ve Yönetim Kurulu İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin hazırlanması-akdedilmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tutulması Zorunlu Defter ve Belgeler	Defter Kapanış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirketler tarafından kullanılan alındı belgeleri, harcama belgeleri ve diğer belgeler)	Kaydedildikleri defterlerdeki sayı ve tarih düzenine uygun olarak 5 yıl süreyle saklanır. Her halde 10 Yıl. (Özel kanunlarda belirtilen süreler saklıdır)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
"GenelİnŞ." Alt Komisyon ve Çalışma Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
"GenelİnŞ." Alt Komisyon ve Çalışma Grupları Toplantı Tutanakları	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş Akdinin Sona Ermesinden ve Dava Açılması Halinde Kesinleşmeden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Log Kayıtları	Kayıt Tarihinden İtibaren 1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan GSM Hattı Kullanım ve Ücret Dökümü	Kayıttan İtibaren 10 Yıl Yargıya İntikal Etmesi Halinde Yargı İşlemleri Saklama Süresine Bkz.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlara Araç Kiralanması Sürecinde Elde Edilen Veriler	İlgili çalışana yönelik kiralama ilişkisi sona erdikten sonraki ilk periyodik imha sürecine kadar muhafaza edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Eğitimleri	İş Güvenliğine Yönelik Alınan Mesleki Eğitim Kayıtları 15 Yıl- Diğerleri 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Özel Sağlık Sigortaları Verileri	Özel Sağlık Sigortasının Koruma Süresinin Bitiminden	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

	itibaren ilk periyodik imha süresine kadar	
Çalışan Adayları Verileri	Başvuru Tarihinden İtibaren 1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Sağlığı ve Güvenliği Mevzuatı kapsamında toplanan veriler	Çalışanlar için iş ilişkisinin sona ermesine müteakip 15 yıl, Tedarikçi çalışanları için ilişkinin sona ermesinden itibariyle 10 yıl.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Stajyer İşlemleri	Stajın sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Burs Yardımı	Burs ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Gezi organizasyonları	Organizasyonun sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Seyahat işlemleri	Seyahat tarihinden sonraki ilk periyodik imza süresine kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Toplantı Katılımcılarının Kaydı	Etkinliğin sona ermesini takiben 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Dijital Arşiv (Etkinlik ve organizasyonlarda edinilen görsel ve işitsel kayıtlar)	Oluşturma tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
"GenelİnŞ." Faaliyetleri Kamera Kayıtları	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mahkeme/icra/idari merciler bilgi taleplerinin cevaplanması ve yargı mercii kayıtlarının tutulması	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Ortağı/Çözüm Ortağı/Danışman ile "GenelİnŞ." 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, "GenelİnŞ." ile 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.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
KVK Süreçleri (Aydınlatma, Açık Rıza, Başvuru ve Şikayetler)	İlgili sürecin tamamlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Silme- Yok Etme- Anonim Hale Getirme Kayıt Süreci	İşlem Tarihinden İtibaren 3 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi Kayıtları	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fihrist ve Rehber Kayıtları	Son iletişim tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Üye Olunan Şirket/Vakıflara ilişkin bilgiler	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatın öngördüğü süre kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Veri Kategorisi Bazında İmha Süreleri **Tablo 5** **İmha , veri saklama süresinin bitimini takip eden ilk periyodik imha süresinde gerçekleştirilecektir.**		
KİŞİSEL VERİ KATEGORİSİ	**KATEGORİZASYON AÇIKLAMASI**	**Veri Saklama Süreleri**
Kimlik Verileri	Gerçek kişilerin kimlik bilgilerine ilişkin kişisel verileri bu kategori altında değerlendirilecektir. (ad soyad, anne - baba adı, anne kızlık soyadı, doğum tarihi, doğum yeri, medeni hali, nüfus cüzdanı seri sıra no, tc kimlik no)	10 Yıl
İletişim Verileri	Kişilerle iletişim amacıyla kullanılabilecek her türlü kişisel veri bu kategori altında değerlendirilecektir. (adres no, e-posta adresi, iletişim adresi, kayıtlı elektronik posta adresi (KEP), telefon no)	10 Yıl
Lokasyon	Bulunduğu yerin konum bilgileri	10 Yıl
Özlük Dosyası Verileri	İlgili mevzuat kapsamında özlük dosyasında bulunan veriler (bordro bilgileri, disiplin soruşturması, işe giriş-çıkış belgesi kayıtları, mal bildirimi bilgileri, izin bilgileri, özgeçmiş bilgileri, performans değerlendirme raporları ve hükümlü başvurularında, ceza mahkumiyetleri ve güvenlik tedbirleri kayıtları (adli sicil kaydı), sağlık bilgileri "Genel olarak özlük dosyalarında aşağıdaki evraklara rastlanmaktadır. 1. Adli sicil kaydı 2. Aile durum bildirimi formu 3. Çalışma Belgesi/Hizmet Belgesi 4. Çok tehlikeli işler için ağır ve tehlikeli işlerde çalışabilir raporu 5. Diploma fotokopisi 6. Doğum izni, çalışabilir/çalışamaz raporları, emzirme izni dilekçeleri, 7. Engelli işçi ise sakatlık raporu, İŞKUR müracaat kayıt belgesi 8. Erkek işçiler için askerlik durumunu gösterir belgeler 9. Eski hükümlü, terör mağduru işçinin İŞKUR müracaat kayıt evrakı 10. Evlilik cüzdanı fotokopisi 11. Fazla çalışmalar için işçi onay yazısı 12. Geçici olarak bir başka işyerine devredilecek işçinin rızasını gösteren belge 13. Haklı fesih varsa bu durumu kanıtlayan belgeler, istifa dilekçesi veya fesih bildirimi 14. İbraname 15. İkametgâh ilmühaberi "16. İş sözleşmesi 17. İşçi hakkında yapılan tüm yazışmalar ve tutulan kayıtlar 18. İşçilerin, iş sağlığı ve güvenliği, mesleki riskler, alınması gerekli tedbirler ve yasal hak ve sorumluluklar konusunda bilgilendirildiklerine dair yazı.	İş akdi sona erdikten sonra 10 Yıl

	19. İşçiye ait bordrolar ve ödemeye ilişkin belgeler 20. İşe giriş ve işten ayrılış bildirgeleri 21. İşe izinsiz gelmeme / iş geç gelme tutanağı ve ihtarname 22. Kan grubu kartı 23. Kıdem ve ihbar tazminatı bordroları 24. Nüfus cüzdanı fotokopisi 25. Nüfus kayıt örneği 26. Özgeçmiş 27. Sağlık raporu ve periyodik sağlık muayene raporları 28. Resim 29. Sağlık Raporu 30. Sakatlık indiriminden yararlanacaklar için Gelir İdaresi Başkanlığından indirim uygulanacağına dair yazı 31. Sigorta olaylarında yapılması gereken idari işlemlere ilişkin (iş kazası tutanağı, iş kazası bildirimi vb.) belgeler 32. Teslim edilen araç gereçler var ise bunların zimmet belgesi 33. Ücretsiz izinler ve yıllık ücretli izin ile ilgili dilekçe, form ve cetveller 34. Varsa almış olduğu eğitim sertifikaları 35. Yabancı işçiler için çalışabilir belgesi 36. Aile durumuna ilişkin veriler İşçi özlük dosyasının bütün bu hususlar göz önünde tutularak işyeri, işin niteliği ve kanuni zorunluluklar dikkate alınarak hazırlanması gerekmektedir. Listede yer almayan ancak kanunen talep edilen bilgi ve belgeler veri sorumlusunun açık rıza olmaksızın işleme faaliyeti kapsamına girmektedir.	
Hukuki İşlem	Adli makamlarla yazışmalar, dava dosyaları, idari takip dosyaları, icra takip dosyaları, davaya dönüşmemiş ihtarname, ihbarname, şikayet, talep, itiraz ve her nevi hukuki bilgi gerektirerek cevaplanması, yazılması gereken bilgi ve belgelerdir.	Söz konusu hukuki işlemin sona ermesinden itibaren 15 Yıl- Özel dava açma süreleri ve işlem süreleri olması halinde ilgili süre dikkate alınacaktır. Adli- İdari makamlarda, dava, takip, süreç devam ettiği süre boyunca kesinleşme, hitam, sona erme nihai olarak tamamlanana kadar süreler kesilmiş-durmuş kabul edilecektir.
Müşteri İşlem	Çağrı merkezi, Santral sistemi kayıtları, fatura, çek, senet, her nevi kıymetli evrak verileri, sipariş bilgisi, talep bilgisi, teklif belgesi, gişe dekontlarıdır.	10 Yıl
Fiziksel Mekan Güvenliği	Çalışan ve ziyaretçilerin giriş, çıkış kayıt bilgileri, kamera kayıtları	2 Yıl – 30 gün
İşlem Güvenliği	IP adres bilgileri, internet sitesi giriş çıkış bilgileri, şifre, parola bilgileri,	1 Yıl
Risk Yönetimi	Ticari, teknik, idari risklerin yönetilmesi için gerekli işlenen bilgiler, veriler	10 Yıl

Finans	Bilanço bilgileri, finansal performans bilgileri, kredi ve risk bilgileri, malvarlığı bilgileri, ayni-nispi mülkiyet hakkı bilgileri, paraya çevrilebilir her türlü araç-türevleri bilgileri	10 Yıl - Özel dava açma süreleri ve işlem süreleri olması halinde ilgili süre dikkate alınacaktır. Adli- İdari makamlarda, dava, takip, süreç, uyuşmazlık, denetim devam ettiği süre boyunca kesinleşme, hitam, sona erme nihai olarak tamamlanana kadar süreler kesilmiş-durmuş kabul edilecektir
Mesleki Deneyim	Diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, transkriptler, cv, özgeçmiş bilgileri	10 Yıl
Görsel İşitsel Kayıtlar	Organizasyon, etkinlik, inceleme, denetim, yönetim kurulu, genel kurul, pay sahibinin hakları dahilindeki faaliyetler, yapılan görüntülü ve sesli kayıtlar ile güvelik amacı ile tutulan görsel/işitsel kayıtlar	10 Yıl- Kaydın alınma amacı dikkate alınarak belirlenecektir. Lütfen Bakınız Tablo 4
Sağlık Bilgileri	Engellilik durumuna ait bilgiler, kan grubu, kişisel sağlık bilgileri, kullanılan cihaz, protez bilgileri ve doktor rapor, tetkik ve belgelerde yer alan her türlü sağlık verisi	10 Yıl
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	Ceza mahkumiyeti, karar verilmesine yer olmadığı, adli sicil kaydı, mahkumiyeti/güvenlik tedbirini içeren mahkeme hükmü belgeleri	10 Yıl
Biyometrik Veri	Avuç içi bilgileri, parmak izi bilgileri, retina taraması bilgileri, yüz tarama bilgileridir.	2 Yıl

5.1. Periyodik İmha Süresi

Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, "GenelİnŞ." KVK Birimince her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11/3 maddesi gereğince, kişisel verileri imha yükümlülüğünün ortaya çıktığı tarihi takip eden **3 ay** içinde kişisel veriler "veri kategorisi durumuna göre silinecek, anonim hale getirilecek ve/veya yok edilecektir.

5.2. Saklama Süresi Sona Eren Kişisel Veriler İçin Gerçekleştirilecek İşlemler

- Kağıt ortamındaki re'sen silme, yok etme veya anonim hale getirme işlemi ilgili birim müdürünün ve Kişisel Verileri Koruma Birimi bilgisi dahilinde ilgili veri kullanıcısı çalışan tarafından, ilgili işlem tutanakla kayıt altına alınmak suretiyle gerçekleştirilir.
- Elektronik ortamdaki re'sen silme, yok etme veya anonim hale getirme işlemi ilgili birim müdürünün ve Kişisel Verileri Koruma Birimi bilgisi dahilinde, bilgi işlem yetkilisince (sunucular, yedekler, yazılımlar, yazıcılar vb. ana veri tabanlarında), söz konusu işlem kayıt altına alınmak sureti ile gerçekleştirilir.
- "GenelİnŞ." Bilgisayar, telefon, e- mail hesabı, tablet vb. ortamda ise ilgili birim müdürünün ve Kişisel Verileri Koruma Birimi bilgisine sunulmak kaydı ile ilgili veri kullanıcısı çalışan tarafından yerine getirilir.
- Çalışanlar,iş için kendisine tahsis edilen bu elektronik ortamlarda gerçekleştirecekleri silme, yok etme işlemlerini envantere uygun şekilde süresinde, KVK Birimini Bilgilendirmek ve Gerekli

tutanağı tutmak suretiyle re'sen gerçekleştirmekle, saklama süresinin dolmasından önce gerçekleşen veri imha sebeplerinde ise KVK Biriminin görüş ve talimatına konuyu bildirmek ve gelecek cevaba uygun şekilde işlemleri gerçekleştirmekle bizzat sorumludur. KVK Birimi Bilgi İşlemden sorumlu üye elektronik ortamdaki bu silme yok etme anonimleştirme işlemlerinin kayıt altına alınması için gerekli teknik donanımı çalışana sağlamakla yükümlüdür.

6. POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

7. VERİ SAHİBİNİN HAKLARI

KVK Kanunu'nun 11 numaralı maddesi kapsamında veri sahiplerine tanınan haklar aşağıda sıralanmaktadır:

- Kişisel veri işlenip işlenmediğini **öğrenme**,
- Kişisel verileri işlenmişse buna ilişkin **bilgi talep etme**,
- Kişisel verilerin işlenme amacını ve bunların **amacına uygun kullanılıp kullanılmadığını** öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin **aktarıldığı üçüncü kişileri** bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların **düzeltilmesini** isteme,
- KVK Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş kişisel verilerin, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde **kişisel verilerin silinmesini veya yok edilmesini isteme** ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

"GenelİnŞ.", her veri sahibinin KVK Kanunu'nun veri sahiplerine tanıdığı hakların rahatça kullanabilmesi konusunda mevzuatın gerekliliklerine uygun olarak gerekli idari ve teknik önemleri almaktadır. Veri sahipleri, yukarıda sayılan haklarını www.genelinsaat.com.tr adresinde yayınlanan ya da "GenelİnŞ." merkezinden temin edebilecekleri başvuru formunu doldurarak aşağıdaki yöntemlerle "GenelİnŞ."a iletebilirler.

Başvuru usulü dahilinde "GenelİnŞ." Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında işlemlerini yürütmektedir. Bu kapsamda başvurunun adı geçen tebliğin 5. Maddesi hükmüne uygun yapılması gerekmektedir.

Form eksiksiz bir şekilde doldurularak;

- "GenelİnŞ." Merkezi'ne yazılı olarak teslim edilebilir,
- İadeli taahhütlü posta ya da noter kanalıyla "GenelİnŞ." adresine gönderilebilir,
- Güvenli elektronik imzayla imzalayarak info@genelinsaat.com.tr adresine e-posta ile iletilebilir,
- Kayıtlı Elektronik Posta (KEP) hesabından genelinsaat@hs06.kep.tr adresine KEP ile iletilebilir.
- İlgili kişi tarafından "GenelİnŞ." e daha önce bildirilen ve "GenelİnŞ." sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle,
- Kurul tarafından belirlenecek diğer yöntemler kullanılabilir.

Başvuruda;

- Ad, soyad ve imza,
- Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası,
- Tebligata esas yerleşim yeri veya iş yeri adresi,
- Varsa bildirime esas elektronik posta adresi, telefon ve faks numarası,
- Talep konusu bulunması zorunludur.
- Konuya ilişkin bilgi ve belgeler başvuruya eklenir.
- Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir.
- Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihidir

"GenelİnŞ.", kişisel veri sahiplerinin yukarıda sıralanan haklarına ilişkin yazılı olarak ya da Kurul tarafından belirlenecek diğer yöntemlerle iletecekleri taleplerini, iletim tarihinden sonra en kısa sürede ve en geç otuz günde sonuçlandıracaktır. Kurul tarafından yayınlanan tarifeler çerçevesinde veri sahiplerinin başvuruları ücretlendirilebilecektir. Adı geçen Tebliğ'in 7. maddesi gereğince, İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

Veri sahipleri tarafından yapılan başvuruların yanıtlanması amacıyla "GenelİnŞ." tarafından başvurucunun kimliğinin doğrulanması ile başvurucu talebinin netleştirilmesi amacıyla ek bilgi ve belge talep edilebilecektir. Söz konusu bilgi ve belgelerin paylaşılmaması halinde veri sahibinin başvurusu cevaplanamayabilecektir.

Başvurunun "kimlik sahibi" ve/veya yetkili kişi tarafından yapılmış olduğunun teyit edilmesi ciddi önem taşımaktadır. Keza amaç kişisel verilerin korunması iken, kimlik doğrulamanın yapılamamasından ötürü 3. kişilere kişisel verilerin verilmesi ve KVK Kanunun 11. maddesinde izah edilen haklar dahilinde işlem yapılması ilgili kişinin korunması gereken menfaatini zedeleyecektir. Bu nedenle kimlik doğrulama işlemleri bakımından hassasiyetimizi anlayışla karşılayacağınızı ve "GenelİnŞ."a yardımcı olacağınızı temenni etmekteyiz.

"GenelİnŞ.", talepleri en kısa sürede ve en geç 30 gün içinde sonuçlandırır. Değerlendirme sonucu yazılı olarak veya elektronik ortamda ilgiliye bildirilir ve talebin kabulü halinde KVK Kanunu'na uygun şekilde gereği yapılır.

Kişisel Veri Sahiplerinin başvurularının reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde ilgili kişi cevabı öğrendiği tarihten itibaren 60 gün içinde Kişisel Verilerin Korunması Kurulu'na KVK Kanunu madde 14 uyarınca şikayette bulunabilir.

8. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

İmha Politikası, "GenelİnŞ." internet sitesinde yayınlanmasının ve/veya tüm çalışanlara duyurulmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, İmha Politikası'nın ıslak imzalı eski nüshaları "GenelİnŞ." Yönetim Kurulu Kararı ile Kişisel Verileri Koruma Birimi tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır.

8.1. Değişiklik Notları