

KİŞİSEL VERİ SAKLAMA İMHA VE ANONİMLEŞTİRME POLİTİKASI

ÖZGÜN İNŞAAT TESİSAT TAAHHÜT TİC.LTD.ŞTİ.

2020 YILI 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU UYUM
ÇALIŞMASI KAPSAMINDA HAZIRLANMIŞTIR.

<https://ozguntaahhut.com/>

1. AMAÇ

Bu Politika; 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca, Şirketimiz bünyesinde işlenen kişisel verilerin saklanması, güvenliğinin sağlanması, imhası (silme-yok etme) ve anonimleştirilmesine ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.

2. KAPSAM

Politika; çalışan, çalışan adayı, taşeron, tedarikçi, ziyaretçi, müşteri ve iş ilişkisi içinde bulunan gerçek kişilere ait tüm kişisel verileri ve bu verilerin bulunduğu tüm kayıt ortamlarını kapsar.

3. DAYANAK

6698 sayılı Kişisel Verilerin Korunması Kanunu

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (28.10.2017)

Aydınlatma Tebliği ve ilgili Kurul kararları

4. TANIMLAR

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

Özel Nitelikli Kişisel Veri: Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep, sendika/dernek üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleri, biyometrik ve genetik veriler.

Kişisel Verilerin İşlenmesi: Kişisel verilerin tamamen/kısmen otomatik yollarla veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi işlemler.

Veri Sorumlusu: ÖZGÜN İNŞAAT TESİSAT TAAHHÜT TİC.LTD.ŞTİ.

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek/tüzel kişi.

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

Periyodik İmha: Kanun'daki işleme şartlarının tamamı ortadan kalktığı anda, Politika'da belirlenen ve tekrar eden aralıklarla resen gerçekleştirilen silme, yok etme veya anonim hale getirme işlemi.

VERBİS: Veri Sorumluları Sicil Bilgi Sistemi.

5. SORUMLULUK VE GÖREVLER

Şirketin tüm birimleri ve çalışanları; kişisel verilerin hukuka uygun elde edilmesi, işlenmesi, saklanması ve imhasında sorumlu birimlere aktif destek sağlar. Kişisel verilere hukuka aykırı erişimin önlenmesi, eğitim ve farkındalıkların sürdürülmesi, denetim bulgularının kapatılması konularında yöneticiler doğrudan sorumludur.

5.1. EK TABLO-1: Saklama ve İmha Süreçleri Görev Dağılımı

UNVANI	BİRİMİ	GÖREVİ
Şirket Müdürü	Şirket	Çalışanların politikaya uygun davranmasından sorumludur.
		Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi İşlem Müdürü	Bilgi İşlem Müdürlüğü	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
	Diğer Tüm Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

6. KAYIT ORTAMLARI

Kişisel veriler aşağıda sayılan ortamlarda güvenli ve mevzuata uygun şekilde muhafaza edilir.

6.1. EK TABLO-2: Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel Bilgisayarlar Mobil Cihazlar Optik Diskler Yazıcılar, Tarayıcılar, Fotokopi Makineleri Çıkarılabilir Ve Taşınabilir Bellekler Sunucular Yazılımlar Bilgi Güvenliği Cihazları	Kağıtlar Yazılı Ve Basılı Ortamlar Görsel Kayıtlar Manuel Veri Kayıt Sistemleri

7. SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirkette, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

- Sözleşmenin kurulması/ifası ile doğrudan ilgili zorunluluklar
- Bir hakkın tesisi, kullanılması veya korunması
- Hukuki yükümlülüklerin yerine getirilmesi (vergi, SGK, İSG, iş hukuku vb.)
- Meşru menfaat (temel hak ve özgürlüklere zarar vermemek kaydıyla)
- Mevzuatta açıkça öngörülmesi
- Açık rızaya dayalı saklama faaliyetleri

8. SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI (Örnekle)

Şirket aşağıdakiler dahil olmak ancak bununla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir:

İnsan kaynakları süreçleri: işe alım, özlük, eğitim, performans, bordro

Kurumsal iletişim ve güvenlik: ziyaretçi/kamera kayıtları, giriş-çıkış (PDKS)

İSG ve acil durum yönetimi: sağlık muayeneleri, kaza kayıtları

Sözleşme ve tedarik zinciri yönetimi

Finans/muhasebe ve yasal raporlama

Hukuki uyumsuzluklarda delil saklama

9. İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Aşağıdaki hallerde kişisel veriler ilgili kişinin talebi üzerine veya re'sen silinir/yok edilir/anonimleştirilir:

- İşleme/saklama amacının ortadan kalkması
- Mevzuat hükümlerinin değişmesi veya kaldırılması
- İşleme faaliyeti açık rızaya dayanıyor ise rızanın geri alınması
- KVKK m.11 kapsamındaki başvurunun kabulü
- Azami saklama süresinin dolması ve daha uzun saklamayı haklı kılan bir sebep bulunmaması

10. TEKNİK TEDBİRLER

- Erişim matrisi ve yetki kısıtlama, güçlü parola ve çok faktörlü kimlik doğrulama
- Şifreleme (disk, yedek, taşınabilir medya), kriptografik koruma
- Ağ güvenliği (GFW, IPS/IDS), uç nokta güvenliği, düzenli patch yönetimi
- Loglama, değişiklik yönetimi ve yedekleme (ayrık ortam)
- Sızma testleri ve zafiyet taramaları; BT risk değerlendirmesi ve iş etki analizi
- İmha işlemlerinde geri döndürülemez yöntemler ve denetim izi kaydı

11. İDARİ TEDBİRLER

- Çalışanlara KVKK ve bilgi güvenliği eğitimleri
- Gizlilik taahhütnameleri ve disiplin prosedürleri
- Taşeron/tedarikçilerle veri koruma hükümleri (SLA/NDA/ek protokol)
- İç denetimler ve uygunsuzlukların giderilmesi
- Veri ihlali tespitinde ilgilinin ve Kurul'un en kısa sürede bilgilendirilmesi

12. KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

12.1. EK TABLO-3: Silme Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortam	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortam	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/ boyanarak/ silinerek karartma işlemi de uygulanır.
Taşınabilir Medya	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

13. KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

13.1. EK TABLO-4: Yok Etme Yöntemleri

Veri Kayıt Ortamı	Yok Etme Yöntemi
Kağıt İmha	Parçalama (cross-cut shredder) ile geri döndürülemez fiziksel imha
Optik/Manyetik Medya sonrası fiziksel yok etme.	Fiziksel delme/eziş, DOD/NIST standartlarında overwrite
Disk/Sunucu kullanılamaz hâle getirme/degaussing	DOD 5220.22-M veya eşdeğeri çoklu üzerine yazım;

14. ANONİMLEŞTİRME YÖNTEMLERİ

Maskeleye: Kimlik alanlarının kısmi/ tam gizlenmesi (örn. TCKN'nin son 4 hanesi).

Toplulaştırma: İstatistik amaçlı grup seviyesinde raporlama.

Genelleştirme: Yaş→yaş aralığı gibi ayrıntı azaltma.

Gürültü Ekleme / Rastgeleleştirme: Tekilleşmeyi engelleyecek veri bozma teknikleri.

15. SAKLAMA VE İMHA SÜRELERİ

Öncelikle mevzuatta öngörülen süreler uygulanır. Mevzuatta süre yoksa, aşağıdaki tablo esas alınır. Süre sonunda 180 gün içinde imha gerçekleştirilir.

15.1. EK TABLO-5: Saklama ve İmha Süresi Tablosu

Süreç	Saklama Süresi	İmha Süresi
İSG uygulamaları (muayene, kaza kayıtları)	İş ilişkisinin bitimini takiben 10 yıl	180 gün
Bordro/ücret, puantaj, izin	İş ilişkisinin bitimini takiben 10 yıl	180 gün
Personel mahkeme/alive talepleri	İş ilişkisinin bitimini takiben 10 yıl	180 gün
Eğitim kayıtları (katılım, sınav)	Eğitimin düzenlenmesini takiben 10 yıl	180 gün
Acil durum hazırlıkları/planları	Hazırlık tarihinden itibaren 10 yıl	180 gün
Log kayıt takip sistemleri	Oluşturulmasından itibaren 10 yıl	180 gün
Kamera kayıtları	6 ay	180 gün
Ziyaretçi kayıtları	2 yıl	180 gün
Tedarikçi/taşeron sözleşmeleri	Sona ermesi takiben 10 yıl	180 gün
Muhasebe/finans evrakı	Vergi mevzuatı gereği 10 yıl	180 gün
İş başvuruları (olumsuz)	6 ay	180 gün

Not: Hukuki uyumsuzluk, denetim veya resmi talep halinde zamanaşımı/yargı süreci bitene kadar saklama devam edebilir.

16. PERİYODİK İMHA TAKVİMİ

Şirketimiz her yıl Haziran ve Aralık aylarında periyodik imha yapar. İmha işlemleri tutanak altına alınır; yöntem, tarih, kapsam ve sorumlular kayıt altındadır.

17. İMHA KAYITLARI VE İSPAT

Her bir imha işlemine ilişkin; veri kategorisi, ortam, yöntem, tarih/saat, sorumlu kişi ve onay bilgileri içeren kayıtlar en az 3 yıl saklanır.

18. VERİ İHLALİ YÖNETİMİ (Özet)

Kişisel verilerin hukuka aykırı yollarla ele geçirilmesi, ifşa olması veya erişilmesi şüphesinde;

- Olay derhâl Bilgi İşlem ve KVKK Sorumlusuna bildirilir.
- Etki analizi yapılır; riskler giderilir.
- Gerekli hâllerde ilgili kişiler ve Kurul mümkün olan en kısa sürede bilgilendirilir.
- Olay ve iyileştirme faaliyetleri tutanak altına alınır.

19. POLİTİKANIN YAYIMLANMASI, SAKLANMASI, GÜNCELLENMESİ

Politika, elektronik ortamda (web sitesi) yayımlanır; ıslak imzalı asıl nüsha şirket bünyesinde saklanır. Mevzuat veya süreç değişikliklerinde güncellenir.

20. YÜRÜRLÜK VE YÜRÜTME

Politika, şirket internet sitesinde yayımlandığı tarihte yürürlüğe girer. Yürürlükten kaldırılması hâlinde eski nüshalar iptal edilerek (kaşe/şerh) en az 5 yıl saklanır. Politikanın yürütülmesinden Üst Yönetim sorumludur.