

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İNFINİTUM BİLGİ SİSTEMLERİ SANAYİ TİCARET LİMİTED ŞİRKETİ

Doküman No	INF-KVK-P02	Yayın Tarihi	06.10.2026
Revizyon	01 (KVYS F.006 Rev.00'ın yerine geçer)	Onaylayan	Şirket Müdürü

1. Amaç

Bu Politika, İNFİNİTUM BİLGİ SİSTEMLERİ SANAYİ TİCARET LİMİTED ŞİRKETİ ("Şirket") tarafından işlenen kişisel verilerin saklanması ve imhasına ilişkin usul ve esasları, 6698 sayılı KVKK m.7 ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca belirlemek amacıyla hazırlanmıştır.

Rev.01 değişiklik özeti: Kamu kurumlarına özgü ifadeler ve mevzuat atıfları (657, 4734, 4982, 3071, 2828 s. Kanunlar, Stratejik Plan, EBYS, çağrı merkezi) çıkarıldı; saklama süreleri şirket süreçlerine göre yeniden belirlendi; log kayıtları için 10 yıllık süre 2 yıla indirildi; kamera kayıtları 30 gün olarak güncellendi; sızma testi verilerine ilişkin imha kuralı genişletildi.

2. Kapsam

Şirket çalışanları, çalışan adayları, stajyerler, müşteri ve potansiyel müşteri yetkilileri, tedarikçi yetkilileri ve çalışanları, ziyaretçiler, web sitesi kullanıcıları, etkinlik ve eğitim katılımcıları ile diğer üçüncü kişilere ait kişisel verilerin işlendiği tüm kayıt ortamları bu Politika kapsamındadır.

3. Tanımlar

Terim	Tanım
Alıcı grubu	Kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kayıt ortamı	Kişisel verilerin bulunduğu her türlü elektronik veya fiziksel ortam.
Kişisel veri işleme envanteri	Şirketin iş süreçlerine bağlı olarak işlediği kişisel verileri; işleme amaçları ve hukuki sebebi, veri kategorisi, alıcı grubu, ilgili kişi grubu, azami saklama süresi, yurt dışına aktarım ve alınan güvenlik tedbirleriyle ilişkilendirerek detaylandırdığı envanter.
Periyodik imha	Kanunda yer alan işleme şartlarının tamamının ortadan kalkması durumunda bu Politikada belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek imha işlemi.
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

4. Sorumluluk ve Görev Dağılımı

Unvan	Birim	Görev
Şirket Müdürü	Üst Yönetim	Politikanın onayı; çalışanların politikaya uygun hareket etmesinin sağlanması; imha tutanaklarının onayı
KVKK Sorumlusu (Refika Barka)	Yönetim	Politikanın hazırlanması, güncellenmesi ve yayımı; periyodik imhanın planlanması ve tutanak altına alınması
BT / Sistem Yöneticisi	BT	Elektronik ortamlardaki imhanın teknik olarak gerçekleştirilmesi; yedeklerin imhası; teknik tedbirler
Birim Yöneticileri (İK, Finans, Satış, Hizmet)	İlgili birim	Birimindeki kayıtların saklama sürelerine uygunluğu; fiziksel evrakın imhaya hazırlanması

Unvan	Birim	Görev
birimleri)		

5. Kayıt Ortamları

Elektronik ortamlar	Fiziksel ortamlar
Microsoft 365 (Outlook, Teams, OneDrive/SharePoint) HubSpot (CRM) Jira ClickUp Paraşüt (ön muhasebe / e-fatura) Kolay İK LinkedIn (işe alım) Şirket içi geliştirilen yazılımlar SIEM / SOC platformu (müşteri log izleme) Uç nokta güvenlik yazılımları (EDR / antivirüs) Dizüstü/masaüstü bilgisayarlar, mobil cihazlar Taşınabilir medya (şifreli USB/harici disk) Yazıcı/tarayıcı hafızaları	Özlük dosyaları (kilitli dolap) Sözleşme ve fatura arşivi Ziyaretçi defteri (varsa) Eğitim katılım formları Basılı raporlar

6. Saklamaya ve İmha ile İlgili Açıklamalar

6.1 Saklamayı gerektiren hukuki sebepler

Kişisel veriler başta aşağıdaki mevzuatta öngörülen süreler boyunca saklanır: 6098 s. Türk Borçlar Kanunu (genel zamanaşımı 10 yıl), 6102 s. Türk Ticaret Kanunu (m.82 - ticari defter ve belgeler 10 yıl), 213 s. Vergi Usul Kanunu (m.253 - 5 yıl), 4857 s. İş Kanunu, 5510 s. Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 6331 s. İş Sağlığı ve Güvenliği Kanunu ve İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği (sağlık dosyası en az 15 yıl), 5651 s. İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun ve ilgili yönetmelikler, 6563 s. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, 7201 s. Tebligat Kanunu ve ilgili diğer mevzuat.

6.2 Saklamayı gerektiren işleme amaçları

İnsan kaynakları süreçlerinin yürütülmesi; sözleşmelerin ifası; finans ve muhasebe yükümlülükleri; bilgi güvenliğinin sağlanması; hukuki uyumsuzluklarda delil olarak kullanılması; yetkili kurumların taleplerinin karşılanması; iş sürekliliğinin sağlanması.

6.3 İmha gerektiren sebepler

Kişisel veriler; işlemeye esas mevzuat hükmünün değişmesi veya kaldırılması, işleme amacının ortadan kalkması, yalnızca açık rızaya dayanan işlemede rızanın geri alınması, ilgili kişinin KVKK m.11 kapsamındaki silme/yok etme başvurusunun kabulü, Kurul kararı veya azami saklama süresinin dolması ve daha uzun saklamayı haklı kılacak bir şartın bulunmaması hallerinde re'sen veya talep üzerine imha edilir.

7. Teknik ve İdari Tedbirler

Kişisel verilerin güvenli saklanması ve hukuka uygun imhası için KVKK m.12 ve Kurulun Kişisel Veri Güvenliği Rehberi çerçevesinde tedbirler alınır. Tedbirlerin ayrıntılı listesi ve uygulama durumu "Teknik ve İdari Tedbirler Kontrol Listesi"nde izlenir. Başlıcaları:

- Teknik:** yetki matrisi ve en az yetki; çok faktörlü kimlik doğrulama; disk şifreleme (BitLocker/FileVault); TLS ile iletim; uç nokta güvenliği (EDR); log yönetimi; yedekleme ve yedeklerin şifrelenmesi; düzenli sızma testi ve zafiyet taraması; güvenli silme araçları.
- İdari:** çalışan gizlilik taahhütnameleri; KVKK eğitimleri; veri işleyen sözleşmeleri; temiz masa/ekran kilidi kuralı; iç denetim; disiplin prosedürü; erişim yetkilerinin işten ayrılıştan önce kaldırılması.

8. İmha Teknikleri

Kayıt ortamı	Yöntem	Açıklama
Sunucu / bulut uygulamaları (Microsoft 365, CRM, İK yazılımı)	Silme	İlgili kayıtlar uygulamanın kalıcı silme fonksiyonuyla silinir; geri dönüşüm kutusu/saklama ilkeleri sonrası kalıcı silme teyit edilir; silme işlemi loglanır.
Veritabanları	Silme / Anonimleştirme	SQL DELETE ve ilgili yedeklerden rotasyonla düşme; istatistik amaçla tutulacak alanlar anonimleştirilir.
Dizüstü/masaüstü, sunucu diskleri	Güvenli silme / Yok etme	Cihaz yeniden kullanılacaksa NIST SP 800-88 uyumlu güvenli silme (crypto-erase); hurdaya ayrılacaksa fiziksel imha (parçalama) ve imha sertifikası.
Taşınabilir medya	Yok etme	Şifreli silme sonrası fiziksel imha.
Kâğıt evrak	Yok etme	Kâğıt kırma makinesinde (en az P-4 seviyesi) geri döndürülemeyecek şekilde imha; büyük hacimde lisanslı imha firması ve tutanak.
Kamera kayıtları	Silme	Kayıt cihazında 30 günlük döngüsel üzerine yazma (otomatik).
Yedekler	Silme	Kaynak veri imha edildiğinde yedekten dönüş engellenir; yedek döngüsü en fazla 1 yılda tamamlanarak veri yedeklerden de düşer.
Analiz/raporlama verileri	Anonim hale getirme	Değişkenleri çıkarma, gruplama/genelleştirme, k-anonimlik gibi yöntemlerle; anonimliğin başka verilerle eşleştirilerek bozulamayacağı kontrol edilir.
Sızma testi / adli bilişim çalışma verileri	Güvenli silme / Yok etme	Rapor SFTP ile teslim edilip teslim teyidi alındıktan sonra en geç 30 gün içinde test cihazlarındaki ham veriler (ekran görüntüleri, hash'ler, dump'lar) güvenli silinir; adli imajlar müşteri talimatına göre iade/imha edilir; imha tutanağı düzenlenir.

9. Saklama ve İmha Süreleri

Kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde, veri kategorisi bazında saklama süreleri VERBİS kaydında, süreç bazında saklama süreleri aşağıdaki tabloda yer alır.

Süreç	Saklama süresi	İmha zamanı
İşe alım ve çalışan adayı değerlendirme	Olumsuz sonuçlanan başvurular: süreç sonundan itibaren 6 ay. Açık rıza ile aday havuzu: 2 yıl. İşe alınan adayın verileri özlük dosyasına aktarılır.	Sürenin bitimini izleyen ilk periyodik imha
Özlük dosyası oluşturma ve işe giriş işlemleri	İş ilişkisinin sona ermesinden itibaren 10 yıl; sağlık dosyası (İSG) en az 15 yıl	Sürenin bitimini izleyen ilk periyodik imha
Bordro, ücret ödemesi ve SGK bildirimleri	Bordro ve ödeme kayıtları: ilgili takvim yılı sonundan itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
İzin, devam ve uzaktan çalışma takibi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Eğitim, sertifikasyon ve performans yönetimi	İş ilişkisinin sona ermesinden itibaren 10 yıl (eğitim gideri taahhüdü kayıtları dahil)	Sürenin bitimini izleyen ilk periyodik imha
Staj programı	Staj bitiminden itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Çalışan bilişim kaynaklarının denetimi ve izlenmesi (uç nokta güvenliği, uzaktan çalışma takibi)	Güvenlik logları 2 yıl; ekran görüntüleri ve aktivite raporları en fazla 3 ay (olay incelemesi halinde süreç sonuna kadar)	Sürenin bitimini izleyen ilk periyodik imha
İş sağlığı ve güvenliği	Sağlık dosyası en az 15 yıl; İSG eğitim kayıtları iş ilişkisi sonrası 10 yıl	Sürenin bitimini izleyen ilk periyodik imha

Süreç	Saklama süresi	İmha zamanı
Zimmet, cihaz tahsisi ve iş çıkışı (offboarding)	İş ilişkisinin sona ermesinden itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Satış, faturalandırma ve tahsilat	Fatura ve defter kayıtları: ilgili hesap döneminin sonundan itibaren 10 yıl (TTK m.82)	Sürenin bitimini izleyen ilk periyodik imha
Tedarikçi kayıtları ve ödemeleri	Hesap dönemi sonundan itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Masraf, avans ve seyahat organizasyonu	Hesap dönemi sonundan itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Potansiyel müşteri (lead) ve müşteri ilişkileri yönetimi (CRM)	Son iletişimden itibaren 2 yıl (sözleşme kurulursa müşteri kaydı süresince + 10 yıl)	Sürenin bitimini izleyen ilk periyodik imha
Teklif ve sözleşme süreçleri	Sözleşmenin sona ermesinden itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Ticari elektronik ileti, e-bülten ve kampanya duyuruları	Onayın geri alınmasından itibaren 1 yıl (onay kayıtları 6563 s. K. gereği 3 yıl)	Sürenin bitimini izleyen ilk periyodik imha
Fuar, etkinlik ve webinar organizasyonu	Etkinlik tarihinden itibaren 2 yıl; tanıtım amaçlı görseller rıza geri alınana kadar	Sürenin bitimini izleyen ilk periyodik imha
Kurumsal web sitesi formları ve ziyaretçi işlemleri	Form kayıtları son iletişimden itibaren 2 yıl; sunucu erişim logları 2 yıl; çerezler - Çerez Politikasındaki süreler	Sürenin bitimini izleyen ilk periyodik imha
Müşteri toplantılarının video/ses kaydı	Proje/teklif sürecinin sonundan itibaren 6 ay	Sürenin bitimini izleyen ilk periyodik imha
Yazılım, lisans ve donanım ürün satışı ile teslimat	Sözleşme/garanti süresinin sonundan itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Sızma testi, Red/Purple Team, zafiyet yönetimi ve CTEM hizmetleri	Rapor müşteriye güvenli kanalla (SFTP) teslim edildikten ve teslim teyidi alındıktan sonra en geç 30 gün içinde ham veriler imha edilir; raporlarda kişisel veriler maskelenir	Sürenin bitimini izleyen ilk periyodik imha
MDR, SOC, OT SOC ve APT tespiti (müşteri log izleme)	Sözleşmede müşteri ile belirlenen süre (önerilen: 12 ay sıcak + 12 ay arşiv); sözleşme sonunda iade/imha	Sürenin bitimini izleyen ilk periyodik imha
Dijital adli bilişim ve olay müdahale ("Saldırı Altındayım")	Müşteri ile belirlenen süre; hukuki süreç varsa süreç sonuna kadar; sonrasında güvenli imha ve imha tutanağı	Sürenin bitimini izleyen ilk periyodik imha
Siber güvenlik / teknoloji eğitimleri ve oltalama (phishing) simülasyonları	Eğitim tarihinden itibaren 2 yıl; sertifika kayıtları 10 yıl; eğitim video kayıtları 6 ay	Sürenin bitimini izleyen ilk periyodik imha
Yazılım test ortamı ve uygulama kullanım logları	Test verisi test süresiyle sınırlı; uygulama logları 2 yıl	Sürenin bitimini izleyen ilk periyodik imha
Proje ve talep yönetimi (Jira, ClickUp)	Proje sonundan itibaren 2 yıl	Sürenin bitimini izleyen ilk periyodik imha
Sistem, ağ ve kod deposu erişim logları	İç IP dağıtım ve erişim logları 2 yıl (5651); diğer sistem logları 2 yıl	Sürenin bitimini izleyen ilk periyodik imha
Kurumsal e-posta, dosya paylaşımı ve iş birliği (Microsoft 365)	İlgili sürecin saklama süresi; ayrılan çalışan posta kutusu ayrılıştan itibaren 6 ay (devir sonrası)	Sürenin bitimini izleyen ilk periyodik imha
Yedekleme ve arşivleme	Kaynak kaydın saklama süresi; yedekler en fazla 1 yıl döngüyle yenilenir	Sürenin bitimini izleyen ilk periyodik imha
Şirketin kendi bilgi güvenliği izlemesi (iç SOC, EDR, SIEM)	2 yıl	Sürenin bitimini izleyen ilk periyodik imha
Ofis kamera (CCTV) kayıtları	30 gün (olay incelemesi gerekirse inceleme/hukuki süreç sonuna kadar)	Sürenin bitimini izleyen ilk periyodik imha
Ziyaretçi giriş kayıtları ve misafir Wi-Fi	Ziyaretçi kaydı 1 yıl; Wi-Fi logları 2 yıl	Sürenin bitimini izleyen ilk periyodik imha

Süreç	Saklama süresi	İmha zamanı
Hukuki süreçler, dava ve icra takipleri	Dosyanın kesinleşmesinden itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Yönetim sistemleri (ISO vb.) denetim ve kayıtları	Denetim döngüsü + 3 yıl	Sürenin bitimini izleyen ilk periyodik imha
İlgili kişi başvurularının alınması ve yanıtlanması	Başvurunun sonuçlanmasından itibaren 10 yıl	Sürenin bitimini izleyen ilk periyodik imha
Kişisel veri imha tutanakları	3 yıl	Sürenin bitimini izleyen ilk periyodik imha

10. Periyodik İmha Süresi

Yönetmelik m.11 uyarınca Şirket periyodik imha süresini **6 ay** olarak belirlemiştir. Periyodik imha her yıl **Haziran** ve **Aralık** aylarında gerçekleştirilir. Yapılan tüm imha işlemleri "Kişisel Veri İmha Tutanağı" ile kayıt altına alınır ve tutanaklar en az 3 yıl saklanır. İlgili kişinin silme/yok etme talebi halinde talep en geç 30 gün içinde sonuçlandırılır.

11. Yayımlama, Güncelleme ve Yürürlük

Politika ıslak imzalı ve elektronik ortamda saklanır, gerekli görülmesi halinde web sitesinde yayımlanır. Politika en az yılda bir gözden geçirilir. Şirket yetkilisinin onayı ile yürürlüğe girer. KVYS F.006 Rev.00 yürürlükten kaldırılmış; ıslak imzalı nüshası "İPTAL" kaşesiyle en az 5 yıl saklanır.