

SAKLAMA VE İMHA POLİTİKASI

1. Amaç

Bu politikanın amacı, Koda Teknoloji Çözümleri A.Ş. tarafından yönetilen bilgi sistemlerinde yer alan verilerin;

- Yasal gerekliliklere uygun sürelerde saklanması
- Gereksiz veri tutulmasının önlenmesini
- Saklama süresi dolan verilerin güvenli şekilde imha edilmesini sağlamaktır.

Bu politika ile veri yaşam döngüsü yönetimi (saklama → arşivleme → imha) güvence altına alınır.

2. Kapsam

Bu politika, aşağıdakileri kapsar.

- Koda Teknoloji Çözümleri A.Ş. tarafından yönetilen tüm sistemler
- Hizmet verilen iştirak şirketlere ait veriler
- Veri tabanları, dosya sistemleri, log kayıtları
- Yedekler ve arşiv ortamları
- Fiziksel ve elektronik veri ortamları

3. Tanımlar

Veri İmha: Verinin geri getirilemeyecek şekilde yok edilmesi

Saklama Süresi: Verinin yasal veya iş gereksinimleri doğrultusunda tutulması gereken süre

Anonimleştirme: Verinin kimlik belirleyici özelliğinin kaldırılması

Kişisel Veri: Kimliği belirli veya belirlenebilir kişiye ait her türlü bilgi

4. Genel İlkeler

- Veriler yalnızca gerekli süre boyunca saklanır
- Yasal saklama sürelerine uyulur
- Süresi dolan veriler güvenli şekilde imha edilir
- İmha işlemleri kayıt altına alınır
- Müşteri verileri ayrı ayrı yönetilir (multi-tenant)

5. Veri Saklama Süreleri

Şirketimiz, kişisel verileri işlendikleri amaç için gerekli olan süre ve ilgili yasal mevzuatta öngörülen en az süre kadar muhafaza etmektedir.

Bu kapsamda, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediği tespit edilmekte, bir süre belirlenmişse bu süreye uygun davranılmaktadır. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır.

Kişisel veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

6. Veri İmha Yöntemleri

6.1 Elektronik Ortam

- Güvenli silme (secure delete)
- Overwrite (üzerine yazma)
- Kriptografik silme

6.2 Fiziksel Ortam

- Disk parçalama (shredding)
- Manyetik yok etme (degauss)
- Fiziksel imha

6.3 Fiziksel Ortam

- Kayıt bazlı silme
- Anonimleştirme
- Arşivleme sonrası imha

7. Yedekler ve Arşivler

- Yedekler de saklama sürelerine tabidir
- Eski yedekler periyodik olarak imha edilir
- Arşivlenen veriler kontrollü erişime açıktır

8. İmha Süreci

- Veri saklama süresi dolduğunda imha süreci başlatılır

- İmha işlemleri yetkili kişiler tarafından yapılır
- İmha işlemleri kayıt altına alınır
- İmha doğrulaması yapılır

9. Uyum

- Veriler yalnızca gerekli süre boyunca saklanır
- Veri minimizasyonu uygulanır
- Veri sahibi talepleri dikkate alınır (Kişisel verilerde)
- Log ve işlem kayıtları mevzuata uygun saklanır (BDDK, KVKK)
- Denetimlerde erişilebilir tutulur
- Veri bütünlüğü korunur

10. Multi-Tenant Veri Yönetimi

- Farklı müşterilere ait veriler ayrı tutulur
- Veri imha süreçleri müşteri bazlı uygulanır
- Veri karışması önlenir

11. Sorumluluklar

Üst Yönetim

- Veri İmha Politikasını onaylar
- Politikaya uyumu sağlar

Tüm İş Birimleri

- Veri saklama ve imha süreçlerini uygular
- Sistemsel kontrolleri sağlar

Bilgi Güvenliği Ekibi

- İmha süreçlerini denetler.
- Sistemsel kontrolleri sağlar.
- İmha kanıtlarını kontrol eder.

12. Uyum, Denetim ve Gözden Geçirme

- İmha işlemleri kayıt altına alınır.
- Denetimlerde sunulmak üzere kanıtlar saklanır.
- Politika periyodik kontroller yapılarak yılda en az bir kez gözden geçirilir
- Gerekli durumlarda güncellenir
- Değişiklikler üst yönetim onayı ile yürürlüğe girer

13. Yürürlük

Bu politika üst yönetim onayı ile yürürlüğe girer.