

Veri İmha Tutanağı / Kaydı

Tutanak No: _____ · Tarih: ____ / ____ / ____

Örnek/taslaktır — hukuki, güvenlik veya KVKK danışmanlığı değildir; kullanmadan önce kendi kurum politikanıza uyarlayın ve gerekiyorsa uzmana danışın.

İmhayı Gerçekleştiren

Kurum / Unvan

Adres

Sorumlu birim / kişi

İletişim

1. İmha Edilen Cihaz / Depolama Ortamları

#	Cihaz / Varlık tanımı	Seri / Etiket No	Medya tipi (SSD/HDD/Teyp)	Hassasiyet	Uygulanan yöntem
1					
2					
3					
4					
5					
6					

2. Uygulanan İmha Yöntemi

- ☐ Yazılımsal güvenli silme (Secure Erase / üzerine yazma) ☐ Kriptografik silme (şifreleme anahtarı imhası)
☐ Degauss (manyetik silme) ☐ Fiziksel imha (parçalama / öğütme / delme) ☐ Diğer: _____

Kullanılan araç / yazılım / hizmet sağlayıcı

İmha yeri

Silme sonucu doğrulandı mı? (yöntem / rapor)

3. KVKK / Kişisel Veri Beyanı

- ☐ İmha edilen cihaz(lar), kişisel veri içeriyordu ve bu veriler yukarıdaki yöntemle geri getirilemeyecek biçimde imha edilmiştir.
☐ Cihaz(lar) kişisel veri içermiyordu.

Not: Kişisel veri içeren cihazlarda imha; ilgili mevzuat ve kurumun saklama/imha politikası dikkate alınarak yapılır. Bu tutanak, imhanın belgelenmesine yardımcı olan bir kayıttır.

İmhayı Gerçekleştiren — Ad, Soyad, İmza

Doğrulayan / Tanık — Ad, Soyad, İmza

Bu belge yalnızca genel bilgilendirme amaçlı bir taslaktır; bağlayıcı bir belge, hukuki görüş, güvenlik ya da KVKK danışmanlığı değildir. Her imha işleminin kendine özgü koşulları vardır. Kullanmadan önce kendi kurum politikanıza uyarlayın ve gerekiyorsa bir uzmana / hukuk danışmanına başvurun. Ücretsiz araç: reyoma.com