Muğla Sıtkı Koçman Üniversitesi

Kurumsal Veri Yönetişim Politikası (Taslak)

Doküman No: MSKÜ-DDVYK-POL-001
Versiyon: 1.0
Hazırlayan: Dijital Dönüşüm ve Veri Yönetimi Koordinatörlüğü
Onaylayan: Üniversite Yönetim Kurulu
Yürürlük Tarihi: …/…/2026

1. Amaç ve Kapsam

Amaç: Bu politikanın amacı, Muğla Sıtkı Koçman Üniversitesi bünyesinde üretilen, kullanılan ve paylaşılan verilerin güvenilir, erişilebilir, doğru, tutarlı ve güncel biçimde yönetilmesini sağlamak; veriye dayalı karar alma kültürünü kurumsallaştırmak ve veri varlıklarını stratejik bir kaynak olarak koruyup geliştirmektir.

Kapsam: Bu politika; Üniversite bünyesindeki tüm akademik ve idari birimlerde yürütülen iş süreçlerinde üretilen veya kullanılan kurumsal verileri, bilgi sistemlerini, veri işleyen tüm personeli ve Üniversite adına veri işleyen üçüncü taraf paydaşları kapsar. Politika hükümleri; öğrenci bilgi sistemleri, personel sistemleri, mali sistemler, araştırma veri tabanları, öğrenme yönetim sistemleri dahil olmak üzere tüm kurumsal bilgi sistemleri için bağlayıcıdır.

2. Temel İlkeler

Veriye Dayalı Yönetişim: Stratejik ve operasyonel karar alma süreçlerinde nesnel, ölçülebilir ve kanıta dayalı veriler esas alınır; sezgisel veya doğrulanamaz bilgiye dayalı kararlar en aza indirilir.

Bütünlük ve Tutarlılık: Veriler sistemler arasında kayıpsız, tutarlı ve standart yapıda korunur; aynı verinin farklı sistemlerde çelişkili biçimlerde yer alması engellenir.

Şeffaflık ve Hesap Verebilirlik: Veri yönetişimi süreçleri şeffaf ve denetlenebilir olmalıdır. Bu kapsamda hangi verinin, kim tarafından ve hangi amaçla işlendiği her zaman kayıt altına alınmalıdır.

Güvenlik ve Sürekli İyileştirme: Veri güvenliği standartlarına uyum sağlanır. 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil mevzuat hükümlerine eksiksiz biçimde uymayı taahhüt eder. Veri yönetim süreçleri periyodik olarak gözden geçirilir. Süreçler, teknolojik gelişmeler, yasal değişiklikler ve kurumsal ihtiyaçlar doğrultusunda güncellenir.

3. Organizasyonel Yapı ve Sorumluluklar

Yönetişim Düzeyi — Dijital Dönüşüm ve Veri Yönetimi Danışma Kurulu: Veri yönetişim politikasının onaylanması, stratejik önceliklerin belirlenmesi ve kurumlar arası veri paylaşım kararlarının alınmasından sorumludur. Politikanın yıllık gözden geçirilmesi bu komisyonun gündemine alınır.

Koordinasyon Düzeyi — Dijital Dönüşüm ve Veri Yönetimi Koordinatörlüğü: Veri yönetişim modelinin işletilmesi, standartların ve prosedürlerin belirlenmesi, veri envanterinin güncel tutulması, birimler arası veri entegrasyon süreçlerinin yönetilmesi ve politikaya uyumun

izlenmesinden sorumludur. Koordinatörlük, bu politikanın birincil uygulama ve geliştirme organıdır.

Operasyonel Düzey — Birim Veri Temsilcileri: Her akademik ve idari birimde, birim yöneticisi tarafından ISO 27001:2022 Bilgi Güvenliği Farkındalık Eğitimini tamamlamış bir Veri Temsilcisi görevlendirilir. Her birim, ürettiği ve kullandığı veri setlerinin doğruluğundan, güncelliğinden ve tanımlı standartlara uygunluğundan sorumludur.

Teknik Düzey — Bilgi İşlem Daire Başkanlığı: Verinin depolanması, yedeklenmesi, siber güvenliğinin sağlanması, teknik altyapının sürekliliği ve erişim yetkilendirme sistemlerinin işletilmesinden sorumludur. Koordinatörlükle teknik konularda düzenli iş birliği içinde çalışır.

4. Veri Yönetim Standartları

4.1. Veri Envanteri

Üniversite bünyesinde üretilen tüm kurumsal veri setleri, Dijital Dönüşüm ve Veri Yönetimi Koordinatörlüğü tarafından yönetilen merkezi bir **Kurumsal Veri Envanteri**'nde kayıt altına alınır. Envanter; her veri setinin adı, kaynağı, sahibi, güncelleme sıklığı, saklama süresi, erişim sınıfı ve bağlı olduğu sistem bilgisini içerir.

4.2. Erişim Yönetimi

Erişim yetkileri, görev değişikliği veya işten ayrılma durumlarında derhal güncellenir. Ayrıcalıklı erişim talepleri yazılı onay gerektir ve kayıt altına alınır.

4.3. Saklama ve İmha

Her veri seti için yasal yükümlülükler ve kurumsal ihtiyaçlar gözetilerek saklama süreleri tanımlanır. Saklama süresi dolan veriler, ilgili mevzuata uygun biçimde belgelenerek imha edilir veya anonimleştirilir.

5. Eğitim ve Farkındalık

Kurumsal veri kültürünün yaygınlaştırılması amacıyla tüm akademik ve idari personele; veri yönetimi standartları, bilgi güvenliği ve kişisel verilerin korunması konularında eğitimler düzenlenir. Yeni göreve başlayan personel, oryantasyon sürecinde bu politika kapsamında bilgilendirilir.

6. Veri İhlali Yönetimi

Veri güvenliği ihlali ya da yetkisiz erişim şüphesi oluştuğunda aşağıdaki süreç işletilir:

İhlali fark eden personel, durumu derhal bağlı olduğu yöneticiye ve Bilgi İşlem Daire Başkanlığı'na bildirir. Bilgi İşlem Daire Başkanlığı, teknik müdahaleyi başlatır ve durumu Dijital Dönüşüm ve Veri Yönetimi Koordinatörlüğü ile Hukuk Müşavirliği'ne raporlar. Kişisel veri içeren bir ihlalin söz konusu olması durumunda, KVKK'nın 12. maddesi uyarınca ihlalden itibaren en geç 72 saat içinde Kişisel Verileri Koruma Kurumu'na bildirim yapılır ve ilgili kişiler uygun yöntemlerle bilgilendirilir. Tüm süreç boyunca alınan önlemler, tespit edilen bulgular ve varılan sonuçlar yazılı olarak kayıt altına alınır.

7. İzleme, Denetim ve Uyum

Dijital Dönüşüm ve Veri Yönetimi Koordinatörlüğü, bu politikanın uygulanmasını yılda en az bir kez değerlendirir ve bulguları raporlar. Kurumsal iç denetim mekanizmaları, veri yönetişim uyumunu denetim kapsamına dahil eder.

Bu politika hükümlerine aykırı davranışlar; ihlalin niteliğine ve büyüklüğüne göre disiplin hükümleri, KVKK yaptırımları veya diğer ilgili mevzuat kapsamında değerlendirilir.