

T.C.
YALOVA ÜNİVERSİTESİ
KURUMSAL VERİ YÖNETİMİ YÖNERGESİ

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönergenin amacı, Yalova Üniversitesinde bütüncül bir yaklaşımla kurumsal veri yönetimini oluşturmak, eğitim-öğretim, araştırma, toplumsal katkı ve sürdürülebilirlik temel alanlarında ve diğer akademik ve yönetsel faaliyetlerde veriye dayalı karar alma süreçlerini güçlendirmek ve veri odaklı stratejik yönetimi sağlamaya yardımcı olmaktır.

Kapsam

MADDE 2- (1) Bu Yönerge, Yalova Üniversitesinin eğitim-öğretim, bilimsel araştırma, araştırma-geliştirme, toplumsal katkı, sürdürülebilirlik ve liderlik, kurumsal yönetim ve kalite temel alanlarında ve kapsama girmeyen diğer alanlarda planlama, uygulama ve operasyonel faaliyetleri yürütme, kontrol etme ve denetleme aşamalarında üretilen verilerin yönetilmesine ilişkin temel politika, ilke rol ve sorumlulukları, veri yönetim döngüsü içerisinde kurumsal veri yönetiminin unsurlarını ve kurumsal veri yönetimine ilişkin kalite standartları ve risk yönetimini kapsamaktadır.

Dayanak

MADDE 3- (1) Bu Yönerge, On İkinci Kalkınma Planında (2024-2028) yer alan Ulusal Veri Stratejisi ve Yalova Üniversitesi Büyük Veri Koordinatörlüğü Yönergesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönergede geçen;

- a) Bilgi İşlem Daire Başkanlığı: Yalova Üniversitesi Bilgi İşlem Daire Başkanlığını,
- b) Hassas veri: Yasal ya da kurumsal nedenlerden dolayı ya da etik sebeple özel bir yetkilendirme olmadan erişilemeyen, ya da yalnızca sınırlı girişe izin verilebilen veri unsurlarını, Kişisel Verileri Koruma Kanunu (KVKK) kapsamında yer alan kişisel verileri, özel nitelikli kişisel verileri ve hasta verileri ile diğer yasalarla, etik yönünden ya da idari yönden sınırlama gerektiren verileri,
- c) Kamusal veri: Kamuya açıklanması Üniversitenin itibarı, kaynakları, hizmetleri veya bireyleri için çok az risk oluşturan veya hiç risk oluşturmayan; anonim haline getirilmemiş kişisel veriler, özel nitelikli kişisel veriler, özel/gizli veriler ve hassas veriler dışında kalan verileri,
- ç) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin doğrudan ya da dolaylı her türlü veriyi,
- d) Kurumsal veri: Üniversitenin planlama, yönetme, faaliyet yürütme, kontrol etme veya denetim faaliyetlerinde doğrudan ya da dolaylı olarak ilgili olan, ürettiği, sahibi olduğu, sakladığı, işlediği ya da paylaştığı veriyi,
- e) Özel nitelikli kişisel veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri ve öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek diğer verileri,



- f) Özel/gizli veri: Yalnızca Üniversitenin ilgili çalışanları tarafından resmi görevleri doğrultusunda gerekli olduğunda erişilebilen verileri,
- g) Üniversite: Yalova Üniversitesini,
- ğ) Üniversite ekosistemi: Üniversitede öğretim elemanı, personel, öğrenci, gönüllü, stajyer, ziyaretçi, Üniversite tarafından sağlanan hizmetler karşılığında herhangi bir ödeme yapılmasına bakılmaksızın mal, hizmet ya da yapım işleri tedarikçisi, dış paydaş ve ilgili diğer kişi ya da kurumu,
- h) Veri: Belirli bir bağlamda anlam taşıyan, gözlemler, ölçümler veya araştırmalar sonucu ya da yönetim bilgi sistemleri ve sosyal medya yoluyla elde edilen ve analiz edildiğinde, yorumlandığında veya organize edildiğinde bilgiye dönüşebilen nicel ya da niteliksel olarak ifade edilebilen anlamlı veri elemanlarından oluşan bilgi parçasını,
- ı) Veri anonimleştirme: Verilerin veriyi tanımlayan kişisel verilerle ya da hassas verilerle ilişkilendirilemeyecek duruma getirilmesini,
- i) Veri elemanı: Kendi başına anlam taşıyan ve verinin alt unsurunu oluşturan ırk, cinsiyet ve lokasyon gibi temel bilgiyi,
- j) Veri kalitesi: Verilerin tanımlanması, doğruluğu, tutarlılığı, entegrasyonu, analizi ve raporlanması gibi unsurların sürekli izlenmesi ve iyileştirilmesini,
- k) Veri kaynağı: Veri tablosunda, veri nesnesinde veya başka bir depolama biçiminde bilgilerin depolandığı fiziksel veya dijital yeri,
- l) Veri seti: Belirli bir hedef ya da gösterge için veya birim tarafından kullanılmak üzere, organize edilmiş verilerin birleşimini,
- m) Veri sızıntısı: Verilerin yasal ve kurumsal düzenlemelere aykırı olarak bilinçli ya da bilinçsiz şekilde değişik yöntemlerle ifşa edilmesini ya da yetkisiz kişiler tarafından ele geçirilmesini,
- n) Veri sözlüğü: Verilere ilişkin üst verilerin tanımlandığı, veri setlerinin ve verilerin künyesinin yer aldığı belgeyi,
- o) Veri tabanı: Genellikle bir bilgisayar sisteminde elektronik olarak depolanan yapılandırılmış bilgilerin ya da verilerin koleksiyonunu,
- ö) Veri yaşam döngüsü: Verinin tanımlanması/oluşturulmasından, yok edilmesine kadar kullanımını içeren döngüyü,
- p) Veri yönetimi: Kurumsal verilerin güvenli bir şekilde toplanması, saklanması ve kullanılmasını içeren uygulama sürecini,
- ifade eder.

İKİNCİ BÖLÜM

Veri Yönetiminde Esas, Temel Politika ve İlkeler

Esaslar

MADDE 5- (1) Verinin yaşam döngüsü içerisinde yönetilmesi, bilgiye dönüştürülmesi ve bilginin paylaşılmasında aşağıdaki düzenlemeler esas alınır:

- a) Kişisel Verileri Koruma Kanunu.
- b) Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

c) Yalova Üniversitesi Kişisel Verileri Koruma Komisyonu Yönergesi.

ç) Yalova Üniversitesi Bilgi Güvenliği Yönetim Sistemi Politikaları.

1) Ek-1: Veri Yönetim Roller ve Veri Seti Matrisi

2) Ek-2: Veri Yönetim Roller ve Sorumlulukları.

(2) Bu düzenlemelerin yanı sıra ulusal düzeydeki yasal düzenlemeler ve bu düzenlemeler doğrultusunda ya da münhasıran Üniversite Yönetim Kurulu ve/veya Üniversite Senatosu tarafından yürürlüğe konulacak yeni düzenlemeler çalışmalarda dikkate alınır.

Temel Politika ve İlkeler

MADDE 6- (1) Veri yönetiminde temel politika ve ilkeler şunlardır:

a) Veri yönetiminin Üniversitenin kurumsal stratejik amaç ve hedefleri ile uyumlu olması sağlanır.

1) Veri, Üniversitenin kurumsal amaç ve hedefleri ile ilişkilendirilir ve bu bağlamda analizleri yapılır.

2) Veri yönetimi ve yapısı fonksiyonel olarak ve kurumsal seviyelerde planlanır.

3) Veri iş odaklı olarak üretilir, kullanılır ve yok edilir.

b) Veri yönetimi ile Üniversitenin stratejik ve operasyonel karar alma süreç ve yetenekleri güçlendirilir.

1) Stratejik ve operasyonel kararların daha sağlıklı ve bilgiye dayalı alınması sağlanır.

2) Akademik performansın izlenmesi için gerekli veriler toplanır, analiz edilir ve sonuçlar ile iyileştirmeye açık alanlar raporlanır.

3) Veri yönetimi, araştırma projelerine destek sağlamak ve yenilikçi çözümler geliştirmek için kullanılabilir.

4) Eğitim ve araştırma kaynaklarının etkin bir şekilde yönetilmesi, bütçe planlaması ve tahsisi gibi süreçlerde veri kullanımı teşvik edilir.

c) Veri yönetimi veri kalite güvencesini sağlayacak nitelikte yürütülür.

1) Veri yönetim sürecinde değerlendirilen veriler, yapılandırılmış ya da yapılandırılmamış nicel, nitel, düzenli, sürekli, ayırık ve zamansal veriler de dahil tüm veri türlerini kapsar.

2) Veriler standardize edilir.

3) Hatalı ve eksik veriler giderilir.

4) Veri elemanlarına ilişkin veri sözlüğü oluşturulur.

5) Her bir veri sahiplenilir ve yönetilir.

6) Verinin bulunabilir, erişilebilir, tutarlı ve yeniden kullanılabilir özelliklerde olması sağlanır.

7) Veri yaşam döngüsüne göre verinin güncelliği korunur.

8) Üniversitenin gelişimine paralel olarak gerektiğinde veri tabanları geliştirilir ve veri mimarisi yeniden oluşturulur.

9) Verilerin yakalanması, depolanması ve muhafaza edilmesinde mükemmellik giderilir.

10) Veri paylaşımı güvenilir ve güvenli bir ortam sağlanarak gerçekleştirilir.

11) Son kullanıcıların verilere erişimi iyileştirilir.

12) Veri yönetiminde risk yönetimi çerçevesinde gerekli iş ve işlemler yerine getirilir, veri kalitesinin iyileştirilmesi için belirlenen kontrol faaliyetleri uygulanır.

13) Veri alan sorumluları tarafından etkin bir şekilde sahiplenilmesi ve yönetilmesini sağlayacak nitelikte veri yönetişim yapısı oluşturulur.

ç) Veri mimarisi ve yönetiminde veri güvenliği ve gizliliğine önem verilir.

1) Veriler yasal ve kurumsal düzenlemelere aykırı olarak, kasıtlı ya da yetkisiz olarak değiştirilmeye, silinmeye, kullanıma ve ifşa edilmeye karşı korunur.

d) Kişisel verilerin işlenmesi kullanılması ve korunmasında veri koruma ilkeleri göz önünde bulundurulur.

1) Kişisel veriler, hukuka uygun bir şekilde işlenir. Veri kaynakları, verilerinin nasıl kullanılacağı konusunda bilgilendirilir.

2) Veri sahiplerinin, verilerine erişim, düzeltme, silme, işleme itirazı gibi hakları bulunur.

3) Kişisel veriler, belirli, açık ve meşru amaçlar için toplanır ve bu amaçlarla sınırlı olarak işlenir.

4) Kişisel veriler, işleme amacına uygun süre boyunca saklanır, bu sürenin sonunda silinir veya anonimleştirilir.

- e) Veriler, yetkisiz erişim, kayıp veya zarar risklerine karşı ilgili düzenlemelerle korunur.
- 1) Kurumsal verileri içeren sistemlerde meydana gelen acil durumlara veya diğer hasar olaylarına müdahale etmek için veri yedekleme, veri kurtarma ve acil durum modu operasyon prosedürlerini içerecek nitelikte acil durum planları oluşturulur.
- 2) Kullanıcının kurumsal verilere erişim yetkisi kullanıcının rolüne bağlı olarak belirli kapsamda ve yetkili kişiler tarafından sağlanır.
- 3) Veri kaynaklarının korunması, veri ihlali, veri sızıntısı ve yetkisiz erişimlere karşı uygun güvenlik politika ve prosedürleri geliştirilir.
- 4) Kurumsal veriler içerisinde hasta verilerine yer verilmez.
- f) Üniversitenin farklı birimleri arasında veri paylaşımı kolaylaştırılır.
- 1) Veri Üniversitenin bir varlığı olarak kabul edilir ve kurumsal kaynak olarak yönetilir.
- 2) Veri bir çalışan, birim ya da sistem tarafından sahiplenilmez.
- 3) Verinin tüm yetkili kullanıcı ve sistemler tarafından erişilebilir halde olması sağlanır.
- 4) Veri farklı sistemler veya kişiler arasında sorunsuz bir şekilde paylaşılabilir.
- g) Veri yönetimi yasal ve kurumsal düzenlemelere uygunluk esasına göre yürütülür.
- 1) Veriler yasal ve kurumsal düzenlemelere uygun olarak kullanılır, gerektiğinde raporlanır ve uygun yöntemlerle paylaşılır.
- 2) Veri yönetim yapısı, veri rolleri ve sorumlulukları açık bir şekilde tanımlanır.
- 3) Kişisel veri, hassas veri ve özel/gizli veriye ilişkin veri yönetim faaliyetleri bu konuda Üniversiteyi bağlayan yasal yükümlülükler ve Üniversitenin kurumsal düzenlemeleri çerçevesinde yürütülür.
- 4) Hassas veriler ve özel/gizli verilerin siber güvenlik önlemleriyle korunması ve yetkisiz kişilerin ve diğer kişi/kurum/tafafların bu verilere erişimini engelleyici düzenlemeler Bilgi İşlem Daire Başkanlığı tarafından yerine getirilir.
- 5) Kişisel verilerin ve kişisel veriler içinde yer alan özel nitelikli kişisel verilerin işlenmesi, silinmesi, yok edilmesi ve anonim haline getirilmesinde KVKK Kanunu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve ilgili diğer mevzuat hükümleri uygulanır.
- 6) Üniversite personelinin Üniversitenin yetki ve sorumluluğu içerisinde yer almayan gizli ve hassas bilgileri elde etme ya da erişmeye çalışması disiplin hükümlerine tabidir.

ÜÇÜNCÜ BÖLÜM

Görev ve Sorumluluklar

Veri sahibi

MADDE 7- (1) Veri sahibi Rektördür. Üniversitenin kurumsal veri yönetiminin üst yöneticisi ve aynı zamanda Üniversite veri yönetiminin başıdır. Veri politika ve ilkelerinin ve veri yönetiminin uygulanmasını sağlar ve veri kalitesini izler.

(2) Veri sahibinin görev ve sorumlulukları şunlardır:

- a) Veri yönetiminin genel strateji ve politikalarının belirlenmesinde liderlik yapar.
- b) Veri yönetim sistemlerinin kurulması ve mevcut altyapının iyileştirilmesi için gerekli kaynağın sağlanması konusunda kararlar alır.
- c) Veri yönetimi için gerekli insan kaynağının ve diğer fiziksel ve mali kaynakların temin edilmesini sağlar.
- ç) Gerekli gördüğünde Veri Yönetim Komisyonu çalışmalarına başkanlık eder.
- d) Veri yönetim kültürünün Üniversitede oluşturulması için eğitim ve farkındalık çalışmalarının yürütülmesini sağlar.
- e) Üniversitede veri güvenliği ve gizliliği konularında yasal ve kurumsal düzenlemelere uygun olarak faaliyetlerin yürütülmesini gözetler.

Veri Yönetim Komisyonu

MADDE 8- (1) Veri Yönetim Komisyonu; Rektör ya da görevlendirilen Rektör Yardımcısı başkanlığında, Akademik Veri Koordinatörü, İdari Veri Koordinatörü, Kurumsal Veri Koordinatörü ve Veri Koruma Yöneticisinden oluşur.

(2) Veri Yönetim Komisyonu, Üniversitede politikalar, planlar ve prosedürler geliştirerek Üniversitenin strateji ve hedefleri doğrultusunda ve yasal ve kurumsal düzenlemeler içerisinde veri yönetiminin yürütülmesinden ve yapılan uygulamaların izlenmesinden sorumludur.

(3) Komisyon, Rektörün ya da Komisyon Başkanının talebi üzerine belirlenen tarihte toplanmak suretiyle çalışmalarını yürütür. Veri Yönetim Komisyonu oy çokluğuyla karar alır.

(4) Veri Yönetim Komisyonunun görev ve sorumlulukları şunlardır:

a) Veri yönetimi ve veri kalitesine ilişkin standartları oluşturur.

b) Yasal ve kurumsal düzenlemeler doğrultusunda Üniversitede veri yönetimi uygulamalarını takip eder.

c) Veri yönetiminde kalitesinin sağlanması ve sürdürülebilirliği için yeni politikalar ve uygulama ilkeleri belirler.

ç) Üniversite ile diğer kurum ve kuruluşlar arasında veri kullanımı ve paylaşımında temel politika ve stratejileri belirler.

d) Raporlanan riskleri, risk eylem planlarını ve varsa kontrol faaliyetlerini değerlendirir ve karara bağlar.

e) Veri yönetiminin etkinliği ve verimliliği için gerekli kararları alır.

Veri Alan Yöneticisi

MADDE 9- (1) Veri Alan Yöneticisi Üniversitenin Rektör Yardımcısı'dır. Yetki ve görev dağılımına bağlı olarak sorumluluğu altındaki birimlerde veri yönetiminin Üniversitedeki veri yönetim düzenlemelerine uygun olarak veri yöneticileri tarafından yürütülmesini sağlamaktan sorumludur.

Veri Yöneticisi

MADDE 10- (1) Üniversitede akademik ve idari birim amirleri Veri Yöneticisidir.

(2) Veri Yöneticisi biriminde verilerin ve veri setlerinin yönetiminin Üniversitedeki veri yönetim düzenlemelerine uygun olarak yürütülmesinden sorumludur.

(3) Veri Yöneticisi birimdeki kurumsal verilerin tamlığı, geçerliliği, güvenilirliği ve zamanlılığından nihai olarak sorumludur. Bu sorumluluğu veri sorumluları ile yerine getirir.

(4) Veri Yöneticisinin görev ve sorumlulukları şunlardır:

a) Akademik, idari ve mali verilerin düzenli, sistematik ve tutarlı bir şekilde toplanmasını sağlar.

b) Toplanan verilerin doğru, eksiksiz ve güncel olmasını temin eder.

c) Faaliyetlerde veri güvenlik ve gizlilik prosedürlerinin uygulanmasını takip eder.

ç) Veri yönetiminin yasal ve kurumsal düzenlemelere uygun şekilde yürütülmesi için biriminde gerekli önlemleri alır.

d) Verilerin depolanması ve erişilebilirliği ile ilgili kararlar alır.

e) Veri yönetiminde diğer birimler ile birimi arasındaki koordinasyonu yürütür.

f) Veri yönetiminin veri kalite prosedürlerine uygun olarak birimde yürütülmesini sağlar.

g) Veri sorumlusu ya da kullanıcıları tarafından veri tabanlarındaki verilere ilişkin sorunları, belirlenen riskleri ve risklere ilişkin kontrol faaliyetlerini Veri Yönetim Komisyonunda görüşülmek üzere Kurumsal Veri Koordinatörlüğüne bildirir.

Akademik/İdari Veri Koordinatörü

MADDE 11- (1) Üniversitede Eğitim-Öğretim, AR-GE, Toplumsal Katkı ve Sürdürülebilirlik Koordinatörlerinin her biri Akademik Veri Koordinatörüdür.

(2) Akademik Veri Koordinatörü, koordinatörlük alanına giren faaliyetlere ilişkin veri setlerini takip etmekten ve veri yönetim sürecinde gerekli rehberlik ve danışmanlık yapmaktan

sorumludur. Akademik Veri Koordinatörleri bu sorumluluklarını kendi faaliyet alanındaki birim koordinatörleri aracılığıyla yerine getirir.

(3) İdari Veri Koordinatörü Genel Sekreterdir. Bu maddenin 2 nci fıkrasında belirtilen ve Üniversite idari ve destek hizmetleri kapsamında yer alan görevlere ilişkin sorumluluklar İdari Veri Koordinatörü tarafından icra edilir.

Kurumsal Veri Koordinatörü

MADDE 12- (1) Kurumsal Veri Koordinatörü Üniversitenin Büyük Veri Koordinatörüdür.

(2) Üniversitede verilerin doğru, güvenli ve kullanılabilir olması için gerekli çalışmaları yürütür, veri yönetiminin belirlenen politika ve düzenlemelere uygun şekilde işletilmesinde veri yönetimindeki sorumlular arasında koordinasyonu sağlar.

(3) Kurumsal Veri Koordinatörü, veri koordinatör yardımcısı ve veri analistleri yardımıyla çalışmalarını yürütür.

(4) Kurumsal Veri Koordinatörünün sorumlulukları şunlardır:

a) Belirli veri setlerine ilişkin üst yönetim ya da Veri Yönetim Komisyonunca talep edilen verilerle ilgili bilgi sağlar.

b) Birimlerden sağlanan veriler doğrultusunda verilerin birleştirilmesini ve gerektiğinde istatistiksel analizini ve raporlamasını sağlar.

c) Üniversitede veri yönetimi süreçlerinin doğru bir şekilde işleminde rehberlik eder.

ç) Veri kullanımına ve veri yönetimine ilişkin birimler tarafından bildirilen riskleri ve kontrol faaliyetlerini Veri Yönetim Komisyonuna sunar.

d) Veri Yönetim Komisyonunca alınan ve Rektör tarafından onaylanan kararların birimlerce uygulanması için gerekli çalışmaları yürütür.

e) Veri tabanlarındaki verilere ilişkin veri yöneticileri tarafından bildirilen sorunları Veri Yönetim Komisyonuna sunar.

Veri Koruma Yöneticisi ve görevlileri

MADDE 13- (1) Veri Koruma Yöneticisi ve görevlileri sırasıyla Üniversitenin Bilgi İşlem Daire Başkanı ve Bilgi İşlem Daire Başkanlığı görevlileridir.

(2) Veri Koruma Yöneticisi Üniversitede veri altyapısının sağlanması ve korunması ile veri sunucu güvenliğinin oluşturulmasından sorumludur. Aynı zamanda, sistem yönetimi, yazılım ve donanım sistem ortamını işletme ve sürdürülebilirliğini sağlama sorumluluğuna sahiptir.

(3) Veri Koruma Yöneticisi ve veri koruma görevlileri aşağıdaki faaliyetleri yürütür:

a) Bilgi işlem sunucularındaki dijital verilerin güvenli bir şekilde saklanması sağlar.

b) Veri güvenliği ve saklama politikasını uygular.

c) Veri tabanı sunucuları, veri depolama çözümleri ve ağ altyapılarını yönetir.

ç) Erişim izinleri ve kullanıcı kimlik doğrulaması için gerekli politikaları uygular.

d) Verilerin güvenliğini sağlamak için şifreleme, güvenlik duvarları ve diğer güvenlik önlemlerini uygular.

e) Verilerin güvenli bir şekilde paylaşılmasını ve transfer edilmesini sağlamak için çözümler sunar.

f) Veri güvenliği ihlallerini tespit eder ve Veri Yönetim Komisyonuna raporlar, bu konuda gerekli önlemleri alır.

g) Verilerin düzenli olarak yedeklenmesini ve yedeklerin güvenli bir şekilde saklanmasını temin eder.

ğ) Veri kaybı durumunda veri kurtarma süreçlerini uygular. Veri güvenliği ve gizliliği konusunda Üniversite personeline eğitimler verilmesini sağlar.

h) Veri tabanı yönetim sistemlerinin bakımını ve güncellenmesini sağlar.

ı) Veri erişim sistemlerinin düzgün çalışmasını denetler.

i) Veri yönetim süreçlerinin sağlıklı yürütülmesi için yerel, ulusal ve uluslararası yasal düzenlemelere uygun olan altyapıları sağlar.

j) Veri Yönetim Komisyonu ya da Kurumsal Veri Koordinatörlüğü tarafından ihtiyaç duyulması halinde büyük veri setlerinin analiz edilmesi, modelleme yapılması veya ileri düzey analizlerin yapılmasını sağlar.

k) Veri tabanlarına ilişkin Veri Yönetim Komisyonu tarafından belirtilen sorunların giderilmesi için gerekli iş ve işlemleri yürütür.

Veri sorumlusu

MADDE 14- (1) Veri sorumlusu Veri Yöneticisi tarafından görevlendirilen kişidir.

(2) Verilerin yaşam döngüsü içerisinde kullanılması ve yönetilmesinden sorumludur. Verilerin toplanması ve korunmasının operasyonel sorumluluğu veri sorumlularına aittir.

(3) Veri sorumlusunun görev ve sorumlulukları şunlardır:

a) Veriyi doğru şekilde toplar, kullanır ve gerektiğinde raporlar.

b) Veri yönetimi, güvenliği ve gizliliği konusunda kurallara uyar.

c) Verilerin doğruluğunu ve güvenilirliğini sağlamak için gerekli önlemleri alır.

ç) Veri kullanımında ve yönetiminde karşılaştığı sorunları, riskleri ve varsa kontrol faaliyeti önerisini Veri Yöneticisine iletir.

Veri kullanıcısı

MADDE 15- (1) Veri kullanıcısı Üniversite ekosistemi üyesidir. Veri kullanıcısı, veri güvenliği ve gizliliğine ilişkin mevcut düzenlemelere uygun olarak veriyi kullanır.

DÖRDÜNCÜ BÖLÜM

Veri Yönetimi ve Veri Yönetiminin Diğer Unsurları

Veri yönetimi

MADDE 16- (1) Veri yönetimi; verinin tanımlanması, toplanması ve korunması, depolanması, doğrulanması ve düzeltilmesi, işlenmesi, analiz edilmesi ve raporlanması adımlarından oluşur.

a) Verilerin tanımlanması:

1) Verinin elde edilebileceği kaynaklar ve bu kaynaklarda yer alan veri elemanları tespit edilerek verinin tanımlanması sağlanır.

2) Verinin nicel veya nitel hangi türde olduğu ve düzenli, yapılandırılmış ya da yapılandırılmamış olduğu tespit edilir.

3) Veri elemanlarının hangi bilgiyi temsil ettiği, hangi stratejik amaç ve hedeflerle ilişkili olduğu belirlenir. Veri elemanlarının bu kapsamda hangi veri içerisinde yer aldığı, verilerin hangi veri setinde bulunduğu karar verilir.

b) Verilerin toplanması ve korunması:

1) Veri sorumlularınca mümkün olduğu kadar veri elemanının ve verinin oluşma noktası ya da kaynağından veri toplanır ve korunur.

2) Her bir manuel ya da dijital yolla veri toplama sürecinde verinin doğruluğu ve güvenliği kontrol edilerek işlem yapılır.

c) Verilerin depolanması:

1) Verinin hangi formatta olduğu belirlenir ve nasıl saklanacağı ve iletileceği tanımlanır. Her bir veri elemanı için veri depolama yeri, veri koruma yöneticisi ve görevlilerince sağlanır.

2) Her bir veri elemanı için veri sorumluları tarafından resmi veri depolama lokasyonlarının kodları tanımlanır.

3) Veri elemanlarının adları, formatları ve kodları verilerin kullanıldığı tüm uygulamalarla uyumlu ve Üniversite veri sözlüğü ile tutarlıdır.

4) Geçmiş verileri saklama ve depolama için arşivleme gereksinimleri veri sorumluları tarafından her bir veri elemanı için tanımlanır.

ç) Verilerin doğrulanması ve düzeltilmesi:

1) Kurumsal verileri yakalayan ve güncel tutan bilgi yönetim sistemleri verilerin doğruluğunu sağlamak için düzeltme ve doğrulama işlemini içerir.

2) Verilerin yetkisiz bir girişimle değiştirilmediği ya da silinmediği, bir lokasyondan diğer lokasyona iletildiğinde verilerin niteliğinin değişmediğini doğrulayan mekanizmalar uygulamaya konulur.

3) Hatalı verilerin yazılı olarak tespit edilmesi ya da bildirilmesi üzerine, mümkün olan en kısa sürede şu düzeltici önlemler alınır: Verilerin hata nedenini düzeltme, verileri resmi depolama yerinde düzeltme, hatalı verilere ulaşan ya da elde eden kullanıcıları uyarma.

d) Verilerin işlenmesi, analiz edilmesi ve raporlanması:

1) Veriler yönetim bilgi sistemlerinde, veri kaynağından doğrudan ya da yetkili kişiler tarafından sisteme giriş yapılarak elde edilir.

2) Verilerde eksik unsurlar giderilir, tutarsızlıklar düzeltilir ve hatalar temizlenir.

3) Veriler belirli bir formata uygun hale getirilir.

4) Veriler kaynağından çıkarılarak sayısal verilere veya gereken niteliğe dönüştürülür.

5) İşlenen veriler çeşitli analiz yöntemlerine tabi tutulur.

6) Elde edilen analiz sonuçları anlaşılır şekilde sunulur.

7) Analiz sonuçları veri görselleştirmeleri ile raporlara dönüştürülür.

8) Kurumsal veri tabanından elde edilen tüm veriler ve tüm raporlamalar verinin elde edildiği zamanı içerir.

9) Veri koruma ve yöneticileri tarafından bilgi yönetim sistemlerinin birimi ilgilendiren veri setleri için veri sorumlularınca veri yöneticilerine, veri yöneticileri tarafından veri alan yöneticilerine ve veri alan yöneticileri tarafından veri sahibine gerçek zamanlı görsel raporların sunulmasına olanak sağlayıcı çözümler geliştirilir.

e) Verilere erişim:

1) Kurumsal veri tabanında bulunan verileri görüntüleme ya da sorgulama izni güvenlik ve gizlilik kuralları ve ilgili yasal düzenlemelere uygun şekilde veri kullanıcılarına sağlanır.

2) Veri tanımlama sürecinin bir parçası olarak, veri yöneticileri her bir veri unsurunu kamuya açık, kişisel, özel nitelikli kişisel, özel/gizli ya da hassas verilerden oluşan kategorilerden birine göre tasnif eder.

3) Kamusal veriler giriş sınırlamasının olmadığı, kamuya açık olabilecek kurumsal veri unsurlarıdır.

4) Üniversite çalışanları yalnızca kendi resmi üniversite görevlerinin performansı için gerekli olduğunda özel/gizli verilere erişmelidir.

5) Gerekli olduğunda, veri yöneticileri bazı veri unsurlarını, veri elemanlarını hassas olarak nitelendirebilir. Hassas veriler veri kullanıcılarının erişimden önce özel yetki alınması gereken veya yalnızca sınırlı bir erişime izin verilen verileri içerir.

6) Verilerin paylaşılması, gizlilik ve güvenlik politika ve ilkelerine uygun olarak icra edilir.

f) Verilerin dokümanite edilmesi:

1) Veri unsurları tanımlanan veriler kaydedilir.

2) Veri dokümantasyonunda veri unsurlarının aşağıdaki özellikleri belirtilmelidir:

- İsmi,

- Kısa tanımı,

- Veri sorumlusu,

- Nerede kullanıldığı,

- Güncelleme sıklığı,

- Veri toplama kaynakları,

- Veri koruma kaynakları,

- Resmi veri depolama yeri ve formatı,

- Hassas, özel/gizli, kamusal ya da açık olarak düzenleme,

- Hassas veri elemanları: sınırlama tanımı/sınıflandırması,

- Doğrulama kriterlerinin ya da düzeltme kontrollerinin tanımı,
- İzin verilen kodların tanımı, anlamı ve lokasyonu,
- Kurallara ve güvenlik gereksinimlerine erişim,
- Arşivleme gereksinimleri.

3) Belgeye dönüştürülen verilerin saklanması, Yükseköğretim Üst Kuruluşları ve Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planı ve Devlet Arşiv Hizmetleri Hakkında Yönetmelik hükümleri uygulanır.

4) Veri unsurları veri sorumluları tarafından gerektiğinde kurumsal veri tabanlarından elde edilir ve belgelendirilir.

g) Kullanıcı desteği:

1) Veri sorumluları sorumlu oldukları veri seti ya da verilerin kullanımında veri kullanıcılarına ve veri girişlerinde diğer veri giriş sorumlularına danışmanlık sağlamalıdır. Ayrıca ilgili verilerin yorumlanması ve anlaşılması için destek olmalıdır. Bu konuda veri yöneticileri tarafından veri sorumlularının eğitim ve farkındalık faaliyetleri desteklenir.

2) Veri tabanlarının kullanımında, verilerin uygun görsel araçlarla sunulmasında veri yöneticileri ve veri sorumluları için Bilgi İşlem Daire Başkanlığı tarafından rehberlik sağlanır.

3) Veri sorumluları eriştikleri veriler kapsamında veri yönetimine ilişkin ilgili düzenlemeleri takip etmek ve uygulamak sorumluluğu altındadır.

ğ) Sistem yönetimi:

1) Kurumsal veriler, esas olarak bütünleştirilmiş tek bir bilgi sistemi içinde tutulur.

2) Yalnızca bilgisayar donanımlarının Üniversitenin genel bilgi sisteminin unsurlarıyla tamamen entegre olması durumunda kurumsal veriler çok sayıda farklı bilgisayar donanımlarında ya da sistemde depolanabilir.

3) Kurumsal verilerin Üniversitenin bilgi sisteminde tek bir lokasyonda tutulması durumunda fiziksel site güvenliği, güvenlik yönetimi ve yetkilendirme sistemleri yedekleme, kurtarma ve sistem yeniden başlatma prosedürleri, veri arşivleme, kapasite planlama ve performans denetimi gibi bilgi güvenliği sorumlulukları sistem yöneticilerine atanır.

h) Veri güvenliği ve felaket kurtarma/iş sürekliliği:

1) Kurumsal veri tabanının kısıtlı bölümlerine girişime sahip olan tüm veri kullanıcıları kendilerine sağlanan erişim düzeylerini ve erişim sağladıkları verilerin gizliliğini koruyacağına ilişkin sorumluluk altındadır.

2) Veri güvenliğinin uygulanmasında Yalova Üniversitesi Bilgi Güvenliği Yönetim Sistemi Politika prosedürleri uygulanır.

3) Veriye erişimi sağlayan bilgi sistemleri spesifik olarak bir kullanıcı ya da birimi belirleyebilme ve erişime izin vermeden önce bazı durumlarda kimlikleri doğrulama özelliklerini sağlamalıdır.

4) Kendisine başvurulduğunda, hassas bilgileri içeren bilgi sistemleri sistem faaliyetleri ve veri erişim incelemelerini desteklemede günlük bazlı işlevli olarak erişim ve faaliyetleri gösterebilmelidir.

5) Depolanır olup olmadığına bakılmaksızın tüm veriler aynı seviyede koruma altında olmalı, hassas veriler şifrelenmelidir.

BEŞİNCİ BÖLÜM

Kurumsal Veri Risk Yönetimi

Kurumsal veri risk yönetimi süreçleri

MADDE 17- (1) Kurumsal veri yönetiminde risk yönetimi, veri ile ilgili risklerin belirlenmesi; riske karşı cevap verilmesi ve iyileştirme planlarının belirlenmesi; değerlendirilmesi ve izlenmesi süreçlerini kapsar.

(2) Kurumsal veri risk yönetiminde yürütülecek faaliyetler şunlardır:

a) Veri kaybı, yetkisiz erişim, veri sızıntısı ve sistem arızaları gibi konularda ve günlük faaliyetlerde karşılaşılan, yasal ve/veya kurumsal düzenlemelere uygun olmayan ya da potansiyel riskler tanımlanır. Aynı zamanda veri yönetim süreçlerinde mevcut zayıflıklar ve eksiklikler belirlenir.

b) Tanımlanan risklerin olasılıkları ve etkileri değerlendirilerek risk skoru hesaplanır.

c) Risk iştahı çerçevesinde ilgili riske karşılık verilecek riske cevap verme yöntemlerinden biri uygulanır.

1) Riskten kaçınma: Belirli risklerin etkisini minimize etmek için süreçlerin değiştirilmesi veya veri kaynaklarının azaltılması, riske dayanak faaliyeti yerine getirmeme,

2) Riskin etkisini azaltmak için başta şifreleme, erişim kontrolleri gibi güvenlik önlemleri ve diğer önlemleri, riski azaltma,

3) Riskin başka bir kuruma/tarafta devredilmesi, riskin transfer edilmesi,

4) Düşük etkili ya da etkisi sınırlı riskler kabul etme, riskin kabul edilmesi.

ç) Riskler sürekli izlenerek, iyileştirme faaliyetlerinin etkinliği düzenli olarak gözden geçirilir ve gerektiğinde değişiklikler yapılır.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Hüküm bulunmayan haller

MADDE 18- (1) Bu Yönergede hüküm bulunmayan hâllerde, ilgili mevzuat hükümleri uygulanır.

Yürürlük

MADDE 19- (1) Bu Yönerge, Üniversite Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 20- (1) Bu Yönerge hükümlerini Yalova Üniversitesi Rektörü yürütür.

Ek-1: Veri Yönetim Roller ve Veri Seti Matrisi

Veri Alanı	Veri Alan Yöneticisi	Akademik/İdari Veri Koordinatörü	Veri Yöneticisi	Veri Sorumlusu	Veri Kullanıcısı
Eğitim ve Öğretim	İlgili Rektör Yardımcısı	Eğitim ve Öğretim Koordinatörü	Dekan Enstitü Müdürü YO Müdürü MYO Müdürü Dış İlişkiler Koordinatörü Kariyer Merkezi Koordinatörü Ortak Dersler Bölümü Başkanı Pedagojik Formasyon Eğitimi Koordinatörü TÖMER Müdürü Uluslararası Öğrenci Birimi Koordinatörü YUZEM Müdürü Öğrenci İşleri Daire Başkanı Personel Daire Başkanı Sağlık Kültür ve Spor Daire Başkanı	Bölüm/Birim Eğitim ve Öğretim Koordinatörü Şube Müdürü Yetkili Personel	Öğretim Elemanı Personel Öğrenci Dış Paydaş İlgili Diğer Kişi, Kurum
Araştırma ve Geliştirme	İlgili Rektör Yardımcısı	AR-GE Koordinatörü	Dekan Enstitü Müdürü YO Müdürü MYO Müdürü YÜMERLAB Müdürü BAP Koordinatörü Kütüphane ve Dokümantasyon Daire Başkanı Döner Sermaye İşletme Müdürü	Bölüm/Birim AR-GE Koordinatörü Şube Müdürü Yetkili Personel	Öğretim Elemanı Personel Öğrenci Dış Paydaş İlgili Diğer Kişi, Kurum
Toplumsal Katkı	İlgili Rektör Yardımcısı	Toplumsal Katkı Koordinatörü	Dekan Enstitü Müdürü YO Müdürü MYO Müdürü TÖMER Müdürü Uygulama Araştırma Merkezi Müdürü YÜSEM Müdürü Sağlık Kültür Spor Daire Başkanı Öğrenci İşleri Daire Başkanı	Bölüm/Birim Toplumsal Katkı Koordinatörü Şube Müdürü Yetkili Personel	Öğretim Elemanı, Personel, Öğrenci, Gönüllü, Stajyer, Ziyaretçi, Dış Paydaş, İlgili Diğer Kişi, Kurum
Liderlik, Yönetişim ve Kalite	İlgili Rektör Yardımcısı	Kalite Koordinatörü Genel Sekreter	Dekan Enstitü Müdürü YO Müdürü MYO Müdürü Uygulama ve Araştırma Merkezi Müdürü Koordinatör İç Denetim Birim Başkanı Genel Sekreter Daire Başkanı Hukuk Müşaviri Döner Sermaye İşletme Müdürü Diğer Akademik ve İdari Birim Yöneticisi	Birim/Bölüm Kalite Koordinatörü Birim/Bölüm Sürdürülebilirlik Koordinatörü Şube Müdürü Yetkili Personel	Öğretim Elemanı, Personel, Öğrenci, Dış Paydaş, İlgili Diğer Kişi, Kurum

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Ek-2: Veri Yönetim Roller ve Sorumlulukları

	Veri Sahibi	Veri Komisyonu	Veri Alan Yöneticisi	Veri Yöneticisi	Akademik/İdari Veri Koordinatörü	Kurumsal Veri Koordinatörü	Veri Koruma Görevlisi	Veri Sorumlusu
Temel sorumluluğu	Stratejik karar alma Politika ve düzenlemeleri onaylama Gözetim	Onaylama Gözden Geçirme İyileştirme	Gözden geçirme İyileştirme Takip etme	Gözden geçirme Takip etme Kullanma Raporlama	Gözden geçirme Takip etme Kullanma Raporlama Eğitim	Koordinasyon Gözden Geçirme İyileştirme Analiz etme Raporlama Eğitim	Veri Koruma Veri güvenliği Veri tabanı işletme ve uygulama Veri Bilgi sistemleri ve Bilgi Teknolojileri sağlama İyileştirme Eğitim	Veri Girişi Veri Toplama Veri Kullanma Veri Saklama Veri Raporlama Veri Belgeleme
Temel İş birliği	Veri Komisyonu Veri Alan Yöneticisi Kurumsal Veri Koordinatörü Veri Koruma Yöneticisi	Veri Sahibi Veri Alan yöneticisi Akademik Veri koordinatörü Kurumsal Veri koordinatörü Veri Yöneticileri Veri Koruma Yöneticisi	Veri Sahibi Veri Komisyonu Veri Yöneticisi Akademik Veri Koordinatörü Kurumsal Veri Koordinatörü Veri Koruma Yöneticisi	Veri Alan Yöneticisi Akademik Veri koordinatörü Kurumsal Veri Koordinatörü Veri Sorumlusu	Veri Alan Yöneticisi Veri Yöneticisi Kurumsal Veri Koordinatörü	Veri Sahibi Veri Komisyonu Veri Alan Yöneticisi Veri Yöneticisi Veri Koruma Yöneticisi Veri Sorumlusu	Veri Sahibi Veri Komisyonu Veri Alan Yöneticisi Veri Yöneticisi Kurumsal Veri Koordinatörü Veri Sorumlusu	Veri Yöneticisi Veri Kullanıcısı
Risk Yönetimi Görevi	Risk yönetimi temel karar ve politikaları onaylama ve gözetim	Konsolide riskleri ve eylem Planlarını onaylama, revize etme	Konsolide risk ve kontrol faaliyetlerini gözden geçirme	Birim riskleri yönetme, risk ve kontrol faaliyetlerini raporlama	Riski ve skorunu belirleme, bildirme	Konsolide risk ve kontrol faaliyetlerini raporlama	Veri güvenlik ve koruma risklerini belirleme ve yönetme	Riski ve skorunu belirleme, bildirme
Veri Raporlama araçları				Toplantılar, Raporlar, Veri yönetim yazılımları üzerinden bilgilendirmeler, Sunumlar	Toplantılar, Sunumlar Veri tabanı raporları, E-posta, Analiz raporları	Toplantılar, Veri tabanı raporları, E-posta, Analiz raporları, Sunumlar	E-posta, Güvenlik ve ihlal bildirimleri, Acil durum raporları Yazılım ve sistem güncellemeleri hakkında duyurular	E-posta, Raporlar, Veri yönetim yazılımları üzerinden bilgilendirmeler
Veri Raporlama Sıklığı		Altı aylık ve gerektiğinde	Haftalık, aylık üç aylık veya gerektiğinde	Haftalık, aylık üç aylık, proje bazlı veya gerektiğinde	Haftalık, aylık üç aylık, proje bazlı veya gerektiğinde	Haftalık, Aylık, üç aylık, proje bazlı gerektiğinde veya analiz raporları talep edildiğinde	Haftalık, aylık, üç aylık, proje bazlı veya gerektiğinde	Haftalık, aylık, üç aylık, proje bazlı veya gerektiğinde

Bu belge, güvenli elektronik imza ile imzalanmıştır.