T.C.
NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Amaç

MADDE 1- (1) Kişisel Verileri Saklama ve İmha Politikası, Üniversitece gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Üniversite tarafından bu doğrultuda hazırlanmış olan bu Politikaya uygun olarak gerçekleştirilir.

Dayanak

MADDE 2- (1) Kişisel Verileri Saklama ve İmha Politikası 07/04/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 28/10/2017 tarihli ve 30224 sayılı Resmi Gazete' de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5 inci ve 6 ncı maddeleri gereğince hazırlanmıştır.

Kapsam

MADDE 3- (1) Kişisel Verileri Saklama ve İmha Politikası 6698 sayılı Kişisel Verilerin Korunması Kanunun da belirtildiği şekilde, Üniversitece tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetleri kapsamaktadır.

Tanımlar

MADDE 4- (1) Bu politikanın uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

b) Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi,

c) Anonim hale getirme: Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

ç) EBYS: Elektronik Belge Yönetim Sistemini,

d) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

e) İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

f) Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

g) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

ğ) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

h) Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

ı) Kişisel veri saklama ve imha tablosu: Kişisel verilerin Üniversite nezdinde tutulacağı süreleri gösteren tabloyu,

i) Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

j) Kişisel verilerin yok edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

k) Kurul: Kişisel Verileri Koruma Kurulu'nu,

l) 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 verilerini,

m) Periyodik imha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,

n) Politika: Niğde Ömer Halisdemir Üniversitesi Kişisel Veri Saklama ve İmha Politikasını,

o) Üniversite: Niğde Ömer Halisdemir Üniversitesini,

ö) VERBİS: Veri Sorumluları Sicil Bilgi Sistemi'ni,

p) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

r) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi (Niğde Ömer Halisdemir Üniversitesini),

s) Yönetmelik: 28/10/2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğini,

ifade eder.

Sorumluluk ve Görev Dağılımları

MADDE 5- (1) Üniversitenin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

(2) Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Rektör	Niğde Ömer Halisdemir Üniversitesi	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması, güncellenmesi ve çalışanların politikaya uygun hareket etmesinden sorumludur.

Bilgi İşlem Daire Başkanı	Bilgi İşlem Daire Başkanlığı	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Daire Başkanları, Hukuk Müşaviri, İç Denetçiler, Dekanlar, Müdürler, Koordinatörler ve Rektörlüğe Bağlı Diğer Birim Yöneticileri	İlgili Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

Politikanın Düzenleme Altına Aldığı Kayıt Ortamları

MADDE 6- (1) Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam, kayıt ortamı kapsamına girer.

(2) Kişisel veriler, Üniversite tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2. Kişisel Verilerin Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
• Sunucular (yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Optik diskler (CD, DVD vb.) • Yazıcı, tarayıcı, fotokopi makinesi • Kamera kayıt sistemleri	• Kâğıt • Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) • Yazılı, basılı, görsel ortamlar

Saklama ve İmhaya İlişkin Açıklamalar

MADDE 7- (1) Üniversite tarafından; çalışanlar, çalışan adayları, öğrenciler, mezunlar, etkinlik katılımcıları, diğer özel kurum veya kuruluşlardan görevli veya araştırmacı, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

7.1.1 Saklamaya İlişkin Açıklamalar

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Üniversitemiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

7.1.2 Saklamayı Gerektiren Hukuki Sebepler

Üniversitemiz faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 2547 sayılı Yükseköğretim Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 2886 sayılı Devlet İhale Kanunu,
- 657 sayılı Devlet Memurları Kanunu,
- 6085 sayılı Sayıştay Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu,
- 4857 sayılı İş Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 18/10/2019 tarihli ve 30922 sayılı Resmi Gazetede yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik,
- Üniversitemiz faaliyetleri kapsamında yürütülen iş ve işlemlere ilişkin kullanılan diğer yasal mevzuat

çerçevesinde, öngörülen saklama süreleri kadar saklanır.

7.1.3 Saklamayı Gerektiren İşleme Amaçları

Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası ile Kişisel Verilerin İşlenmesi Hakkında Aydınlatma Metninde belirtilmiştir.

7.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya mülgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Üniversite tarafından kabul edilmesi,
- Üniversitenin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması durumlarında, Üniversite tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

Teknik ve İdari Tedbirler

MADDE 8- (1) Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli

kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Üniversite tarafından teknik ve idari tedbirler alınır.

8.1.1 Teknik Tedbirler

Üniversite tarafından, işlediği kişisel verilerle ve özel nitelikli kişisel verilerin saklanması için asgari olarak aşağıdaki tedbirler alınır.

- Sızma (Penetrasyon) testleri ile Üniversitemiz bilişim sistemlerine (Sunucular, bilgi güvenliği cihazları) yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin (Sunucular, bilgi güvenliği cihazları) sürekliliğini etkileyecek riskler ve tehditler izlenir.
- Üniversite tarafından geliştirilen yazılımlar ile EBYS' de kullanıcıların yetkilendirilmesi, için kurallar oluşturulur.
- Üniversite bilişim sistemleri (Sunucular, bilgi güvenliği cihazları) teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınır.
- Çevresel tehditlere karşı bilişim sistemleri (Sunucular, bilgi güvenliği cihazları) güvenliğinin sağlanması için, sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yangın söndürme sistemi, iklimlendirme sistemi vb. önlemler alınır.
- Bilişim Sistemlerine (Sunucular, bilgi güvenliği cihazları) ait dış tehditleri önlemek amacıyla güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb. önlemler alınır.
- Üniversite tarafından, bilgisayar ve mobil cihazlar için zararlı yazılımları engelleyen antivirüs yazılımı temin edilir.
- Üniversite bilişim sistemlerinin (Sunucular, bilgi güvenliği cihazları) bulunduğu saklama alanlarına fiziksel erişimler kayıt altına alınır.
- Kişisel verilerin işlendiği Üniversite bilişim sistemlerinde (Sunucular, bilgi güvenliği cihazları) güçlü parolalar kullanılır.
- Bilişim Sistemleri (Sunucular, bilgi güvenliği cihazları) üzerinden silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirler alınır.
- Bilişim sistemlerinde (Sunucular, bilgi güvenliği cihazları) güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenir ve bilgi sistemleri güncel halde tutulur.
- Üniversite bilişim sistemlerinde (Sunucular, bilgi güvenliği cihazları) güvenli kayıt tutma (loglama) sistemleri kullanılır.
- Üniversite Bilişim sistemlerinde (Sunucular, bilgi güvenliği cihazları) verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılır.
- Üniversite internet sayfasına erişimde güvenli protokol (HTTPS) kullanılır.
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında güvenli veri aktarımıyla gerçekleştirilir.
- Kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise; kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerini (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alır, yetkisiz giriş çıkışları engeller.
- Özel nitelikli kişisel veriler aktarılacaksa; aktarma işlemi evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınır ve evrak "Gizli ” formatta gönderilir.

- Kişisel veri bulundurulan tüm elektronik cihazlar, bu cihazları kullanan çalışanlar tarafından çevresel tehditlere karşı korunur.
- Kişisel veri bulundurulan tüm elektronik cihazlarda, bu cihazları kullanan çalışanlar tarafından güçlü parolalar kullanılır.
- Kişisel veri bulundurulan tüm elektronik cihazlar, bu cihazları kullanan çalışanlar tarafından, kullanılmadıkları durumlarda otomatik olarak ekran korumasına geçecek şekilde ayarlanır ve mesai bitiminde kapatılır.
- Çalışanlar tarafından kişisel veri bulunan tüm elektronik cihazları yetkili personel dışındaki kişilerce kullanılması engellenir.
- Kişisel veri bulunan tüm bilgisayarın kullanıcıları tarafından Üniversitenin sağladığı lisanslı antivirüs yazılım ve modüller yüklenir. Antivirüs yazılımı yüklü olmayan cihazlar ağa bağlanmaz.
- Kişisel veri bulunan taşınabilir cihazlar çalınma riskine karşı kullanıcılar tarafından gözetimsiz bırakılmaz ve bu cihazların fiziksel güvenliği sağlanır ve bu cihazlarda hassas ve gizli bilgiler mümkün olduğunca bulundurulmaz.

8.1.2 İdari Tedbirler

Üniversite tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Personele, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili diğer mevzuat hakkında eğitimler verilir.
- Üniversite tarafından yürütülen faaliyetlere ilişkin personel ile gizlilik sözleşmesi imzalanır.
- Kişisel veri işlenmeye başlamadan önce, Üniversite tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilir.
- Kişisel veri işleme envanteri hazırlanır.
- Üniversite içi denetimler yapılır.
- Personele bilgi güvenliği eğitimleri verilir.

(2) Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan personele yönelik; Üniversite, özel nitelikli kişisel veri güvenliği konularında eğitim düzenleyerek farkındalığın artmasını sağlar, personel ile gizlilik sözleşmeleri yapar, verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarını ve süreleri net olarak tanımlar, periyodik olarak yetki kontrolleri gerçekleştirir, görev değişikliği olan ya da Üniversiteden ayrılan personelin bu alandaki yetkilerini derhal kaldırır.

Kişisel Verileri İmha Teknikleri

MADDE 9- (1) İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Üniversite tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

9.1.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama

Elektronik Ortamda (sunucu, veri tabanı, bilgi güvenliği cihazlarında) Yer Alan Kişisel Veriler	Elektronik ortamlarda yer alan kişisel verilerden saklama süresi sona erenler, ilgili sistem yöneticisi tarafından, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Diğer Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamın sahibi/kullanıcısı tarafından silinir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklama süresi sona erenler, evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

9.1.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Üniversite tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklama süresi sona erenler, geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklama süresi sona erenler için eritme, yakma veya toz haline getirme gibi fiziksel olarak yok etme işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

9.1.3 Kişisel Verilerin Anonim Hale Getirilmesi

(1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

(2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilir.

Saklama ve İmha Süreleri

MADDE 10- (1)Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamında saklama süreleri Kişisel Veri İşleme Envanterinde, Veri kategorileri bazında saklama süreleri ise VERBİS'te yer alır. Söz konusu saklama süreleri üzerinde, gerekmesi halinde Üniversite güncellemeler yapar.
Saklama süresi tespitinde söz konusu veri işlemi hakkında mevzuatta bir saklama süresi öngörülmüş ise öncelikle bu süreye riayet edilir.

(2) Saklama süreleri sona eren kişisel verileri re'sen silme, yok etme veya anonim hale getirme işlemi, sunucular, veri tabanları, bilgi güvenliği cihazları için Bilgi İşlem Daire Başkanlığı tarafından, diğer elektronik ortamlar ile elektronik olmayan ortamlardaki kişisel veriler için ilgili birimler tarafından yerine getirilir.

(3) Kişisel veriler aksine kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça; genel dava zamanaşımı süresini düzenleyen 6098 sayılı Türk Borçlar Kanunu'nun 146 ncı maddesi gereği 10 yıl, ilgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü gerektiren mevzuat kapsamında bir suça konu olması veya bir suç ile ilişkili olması durumunda 5237 sayılı Türk Ceza Kanunu'nun 66 ncı ve 68 inci maddeleri gereği dava zamanaşımı ve ceza zamanaşımı ile ve 5352 sayılı Adli Sicil Kanunu'nda belirtilen süreler saklı kalmak kaydıyla; kişisel veri işleme envanterinde belirtildiği sürede saklanır ve saklama süresinin bitimini takip eden ilk periyodik imha süresinde ilgili mevzuat çerçevesinde imha edilir.

(4) Veri kategorilerine göre saklama sürelerini gösteren tablo aşağıda verilmiştir.

SAKLAMA SÜRECİ	
VERİ KATEGORİSİ	YIL/AY/GÜN
Kimlik	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
İletişim	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Lokasyon	
Özlük	Süresiz
Hukuki İşlem	Süresiz
Müşteri İşlem	10 YIL
Fiziksel Mekan Güvenliği	1 AY
İşlem Güvenliği	2 YIL
Risk Yönetimi	10 YIL
Finans	10 YIL
Mesleki Deneyim	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Pazarlama	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Görsel Ve İşitsel Kayıtlar	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Irk Ve Etnik Köken	
Siyasi Düşünce Bilgileri	
Felsefi inanç,din,mezhep ve diğer inançlar	
Kılık ve Kıyafet	
Dernek üyeliği	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Vakıf Üyeliği	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Sendika Üyeliği	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Sağlık Bilgileri	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Cinsel Hayat	
Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında Öngörülen Sürelerle Saklanmaktadır.
Biyometrik Veri	Çalışma ve Öğrencilik İlişkisi Devam Ettiği Sürece Saklanmaktadır.
Genetik Veri	

Peryodik İmha Süresi

MADDE 11- (1) Yönetmeliğin 11 inci maddesi gereğince Üniversite, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Üniversite her yıl Haziran ve Aralık aylarında periyodik imha işlemini gerçekleştirir. İmha işlemi ve imhanın içeriği ilgili birim tarafından tutanak altına alınır.

Politika'nın Yayınlanması ve Saklanması

MADDE 12- (1) Politika, internet sayfasında kamuya açıklanır. Bir nüshası Personel Daire Başkanlığı'nda saklanır.

Yürürlük

MADDE 13- (1) Politika, Üniversite Senatosunun onayından sonra yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu politika Rektör tarafından yürütülür.