KARADENİZ TEKNİK ÜNİVERSİTESİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1-AMAÇ

Kişisel Verileri Saklama ve İmha Politikasının amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu 7. Maddesine istinaden çıkarılan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" 5. ve 6. Maddeleri uyarınca Karadeniz Teknik Üniversitesi tarafından işlenen kişisel verilerin, saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Karadeniz Teknik Üniversitesi tarafından bu doğrultuda hazırlanmış olan Kişisel Veri Saklama ve İmha Politikasına uygun olarak gerçekleştirilir.

2-KAPSAM

Bu politika, kurum çalışanlarımız, çalışan adaylarımız, öğrencilerimiz ve öğrenci adaylarımız, hizmet sağlayıcılarımız, ziyaretçilerimiz, kurum ile hukuki ilişki içinde olan gerçek ve tüzel kişiler ile üçüncü kişilerin otomatik olan veya otomatik olmayan yollarla işlenen bütün kişisel verilerini kapsamaktadır.

3- DAYANAK

7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.

4-TANIMLAR

Açık Rıza : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
Alıcı Grubu : Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
Anonim Hale Getirme : Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
Çalışan : Karadeniz Teknik Üniversitesi çalışanlarını,
Daire Başkanı : Karadeniz Teknik Üniversitesi Daire Başkanlarını,
Dekan: 2547 sayılı Kanun'un l6'ncı maddesine istinaden atanan öğretim üyesini,
Döner Sermaye İşletmesi Müdürlüğü : Karadeniz Teknik Üniversitesi Döner Sermaye İşletmesi Müdürlüğü'nü
Döner Sermaye İşletme Müdürü: Karadeniz Teknik Üniversitesi Döner Sermaye İşletme Müdürünü,
Elektronik Ortam : Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,
Elektronik Olmayan Ortam : Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel ve diğer ortamları,
Fakülte : Karadeniz Teknik Üniversitesi'ne bağlı fakülteleri,
Hukuk Müşaviri: Karadeniz Teknik Üniversitesi Hukuk Müşavirini,
Hukuk Müşavirliği: Karadeniz Teknik Üniversitesi Hukuk Müşavirliğini,
İlgili Kişi : Kişisel verisi işlenen gerçek kişiyi,

İlgili Kullanıcı : Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,
İmha : Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kanun : 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,
Kayıt Ortamı : Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,
Koordinatör : Karadeniz Teknik Üniversitesi bünyesinde yer alan Koordinatörlüklerden sorumlu gerçek kişileri,
Kişisel Veri : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
Kişisel Verilerin İşlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul : Kişisel Verileri Koruma Kurulunu,
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,
Periyodik İmha : 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,
Politika : Kişisel Verileri Saklama ve İmha Politikasını,
Veri İşleyen : Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
Üniversite: Karadeniz Teknik Üniversitesini,
Üniversite Yönetim Kurulu (ÜYK) : Karadeniz Teknik Üniversitesi Yönetim Kurulu'nu,
Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişiyi,
Yönetmelik : Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği,
Yüksekokul : Karadeniz Teknik Üniversitesi'nde bulunan Yüksekokulu,
Yüksekokul Müdürü : Karadeniz Teknik Üniversitesi'nde bulunan Yüksekokul Müdürünü ifade eder.

5- KİŞİSEL VERİLERİN SAKLANMASI ve İMHASI İÇİN DÜZENLENEN KAYIT ORTAMLARI

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. Üniversite bünyesinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize göre;

Kağıt Ortamlar;

- Kağıt
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri),
- Yazılı, basılı ve görsel ortamlar.

Elektronik Ortamlar;

- Ms Office Dosyaları,
- Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
- Sunucularımız,
- Yazılımlarımız,
- Antivirüs programları ve güvenlik duvarı ile hassas bir şekilde korunan Bilgisayarlarımız,
- Ağ cihazlarımız,
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri,
- Üniversitemize ait Bulut sistemleri,
- Mobil telefonlar ve içerisindeki tüm saklama alanları,
- Çevre birimler (parmak izi okuyucu, yazıcı),

belirtilen kayıt ortamlarında güvenli bir şekilde saklanır.

6- KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Üniversite bünyesinde bulunan kişisel veriler, eğitim ve araştırma faaliyetlerinin kesintisiz olarak sürdürülmesi, hizmetlerin sunulması, hukuki yükümlülüklerinin yerine getirilmesi, çalışan haklarının planlanması ve yerine getirilmesi amacıyla aşağıda yer alan veri işleme sebepleriyle elektronik veya fiziki ortamlarda güvenli bir şekilde Kanun ve ilgili yönetmelikte belirtilen sınırlar dahilinde saklanmaktadır. Aşağıda belirtilen sebeplerin ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine de imha edilmektedir.

- Açık rızanın varlığı,
- Kanun hükmünün varlığı,
- Fiili imkânsızlık nedeniyle açık rızanın alınamaması,
- Sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kişisel verisinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşuluyla veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması.

7- KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Üniversite, 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 aşağıda yer alan teknik ve idari tedbirleri almaktadır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.
- KTÜ makamları bilişim kaynaklarının aykırı etkinlikler dahilinde kullanılması durumunda KTÜ Bilgisayar, Ağ ve Bilişim Kaynakları Kullanım Yönergesi 24. Madde kapsamında işlemleri tahsis edecektir.
- Çalışanların niteliğinin geliştirilmesine yönelik, 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 ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

8- KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Bu politikanın 5. maddesinde belirtilen şartların ortandan kalkması halinde, kişisel veriler Üniversite tarafından kendiliğinden veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta ilgili kişi tarafından Üniversite'ye başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlanır ve ilgili kişiye bilgi verilir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir,
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri kendiliğinden silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilir. Ancak, ilgili kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilir.

Üniversite, kişisel verileri imha etmeye (silmeye, yok etmeye ve anonim hale getirmeye) yönelik uygulamaları aşağıda belirtildiği şekilde uygulamaktadır.

Kişisel Verilerin Silinmesi

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.
- Merkezi sunucuda yer alan ofis dosyaları, dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması ile gerçekleştirilmektedir.
- Taşınabilir medyada bulunan kişisel veriler flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve veri silineceği zaman tekrar geri getirilemeyecek şekilde biçimlendirilir.
- Veri tabanlarında bulunan kişisel veriler, ilgili satırların/sütunların ya da tablo içerisinde yer alan hücreler veri tabanı komutları ile (DELETE vb.) silinmektedir.
- Kurum bilgisayarlarında bulunan kişisel verilere kimlik doğrulama ile erişim sağlanmakta ve işletim sistemi komutları kullanılarak silinmektedir.

Kişisel Verilerin Yok Edilmesi

- Yerel sistemler üzerindeki kişisel verilerin yok edilmesi; de-manyetize etme (medyanın özel bir cihazdan geçirilerek yüksek bir değerde manyetik alana maruz bırakılması), fiziksel yok etme (Medya ve manyetik medyanın eritilmesi, yakılması, öğütücülerin kullanılması) ve üzerine yazma yöntemiyle yok edilmektedir.
- Çevresel sistemler üzerindeki kişisel verilerin yok edilmesi; Ağ cihazları (switch, router vb.), Flash tabanlı ortamlar/sabit disklerin (ATA "SATA, PATA vb.", SCSI "SCSI Express vb.), Manyetik bant, Manyetik disk gibi üniteler, Mobil telefonlar (Sim kart ve sabit hafıza alanları), Veri kayıt ortamı çıkartılabilir ya da sabit olan yazıcı ve parmak izli kapı geçiş sistemi gibi çevre birimler, Optik diskler olarak belirtebileceğimiz çevresel kayıt sistemleri dijital ortam ise ürün özelliği olarak destekleniyorsa gibi yok etme komutunu kullanmak, dijital ortamın ürün özelliği olarak desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da "de-manyetize etme, fiziksel yok etme, üzerine yazma" olarak belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak, son olarak dijital ortam değil ise "demanyetize etme, fiziksel yok etme, üzerine yazma" yöntemlerin uygun bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- Kâğıt ve mikro ofis ortamlarında bulunan kişisel veriler bulunduğu kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan, bu verilerin bulunduğu ana ortamın yok edilerek imha işlemi gerçekleştirilmektedir.

- Bulut ortamında bulunan kişisel veriler şifrelenerek saklanmakta ve imha süresi geldiğinde yok etme komutu uygulanmaktadır.

Kişisel Verilerin Anonim Hale Getirilmesi

- Maskeleme yöntemi ile veri sahibinin tanımlanmasını sağlayan temel belirleyici bilgiler (örn: isim, soyisim, TCKN) çıkartılarak anonimleştirme gerçekleştirilmektedir.
- Toplulaştırma yöntemi ile kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek bir şekilde (örn: 25 ile 30 yaş aralığındaki kişilerden gelen iş başvurusunun daha fazla olması) çıkartılarak anonimleştirme gerçekleştirilmektedir.
- Veri Türetme yöntemi ile kişisel verilerin içeriğinden daha genel bir içerik oluşturularak ve kişisel verinin herhangi bir şekilde bir kişiyle bağdaştırılamayacak şekilde (örn: doğum tarihleri yerine yaş yazılması) anonim hale getirme gerçekleştirilmektedir.

9- KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

<table>
<tr><th>Unvan</th><th>Birim</th><th>Görev</th></tr>
<tr><td>Rektör</td><td>Karadeniz Teknik Üniversitesi</td><td>Çalışanların politikaya uygun hareket etmesinden sorumludur.</td></tr>
<tr><td>Sorumlu Rektör Yardımcısı</td><td>Karadeniz Teknik Üniversitesi</td><td>Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi ile uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.</td></tr>
<tr><td>Dekan</td><td>Fakülte</td><td rowspan="9">Politikanın görev alanları kapsamında yürütülmesinden sorumludur.</td></tr>
<tr><td>Enstitü Müdürü</td><td>Enstitü</td></tr>
<tr><td>Yüksekokul Müdürü</td><td>Yüksekokul</td></tr>
<tr><td>Meslek Yüksekokul Müdürü</td><td>Meslek Yüksekokul</td></tr>
<tr><td>Merkez Müdürü</td><td>Uygulama ve Araştırma Merkezi</td></tr>
<tr><td>Koordinatör</td><td>Koordinatörlükler</td></tr>
<tr><td>Daire Başkanı</td><td>Daire Başkanlıkları</td></tr>
<tr><td>Döner Sermaye İşletme Müdürü</td><td>Döner Sermaye İşletme Müdürlüğü</td></tr>
<tr><td>Hukuk Müşaviri</td><td>Hukuk Müşavirliği</td></tr>
<tr><td>Arşiv Sorumlusu</td><td></td><td>Kişisel verilerin imha edilmesi</td></tr>
<tr><td>Bilgi İşlem Personeli</td><td></td><td>Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması</td></tr>
</table>

İdari İşler Personeli		Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması

10- KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜRELERİNE İLİŞKİN TABLO

Üniversite bünyesinde bulunan kişisel veriler; ilgili kanunlarda ve mevzuatta öngörülmesi durumunda bu mevzuatta belirtilen süre boyunca saklamaktadır.

SAKLANAN KİŞİSEL VERİLER	SAKLAMA SÜRESİ	İMHA SÜRESİ
1-Kimlik Adı-soyadı, anne-baba adı, anne kızlık soyadı, doğum tarihi, doğum yeri, medeni hali, nüfus cüzdanı seri sıra numarası, T.C. kimlik numarası vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir
2-İletişim Adres numarası, e-posta adresi, iletişim adresi, kayıtlı elektronik posta adresi (KEP), telefon numarası vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir
3-Lokasyon Bulunduğu yerin konum bilgileri vb.	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
4-Özlük Bordro bilgileri, disiplin soruşturması, işe giriş belgesi kayıtları, mal bildirimi bilgileri, özgeçmiş bilgileri, performans değerlendirme raporları vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
5-Hukuki işlem Adli makamlarla yazışmalardaki bilgiler, dava dosyasındaki bilgiler vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
6-Müşteri işlem Çağrı merkezi kayıtları, fatura, senet, çek bilgileri, gişe dekontlarındaki bilgiler, sipariş bilgisi, talep bilgisi vb.	3 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
7-Fiziksel mekân güvenliği Çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri, kamera kayıtları vb.	3 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
8-İşlem güvenliği IP adresi bilgileri, internet sitesi giriş çıkış bilgileri, şifre ve parola bilgileri vb.	3 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
9-Risk yönetimi Ticari, teknik, idari risklerin yönetilmesi için işlenen bilgiler vb.	15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
10-Finans Bilanço bilgileri, finansal performans bilgileri, kredi ve risk bilgileri, malvarlığı bilgileri vb.	15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

10-Mesleki deneyim Diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, transkript bilgileri vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
11-Görsel ve işitsel kayıtlar görsel ve işitsel kayıtlar vb.	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
12-Dernek üyeliği, Dernek üyeliği bilgileri vb.	Faaliyet Süresi + 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
13-Vakıf üyeliği, Vakıf üyeliği bilgileri vb.	Faaliyet Süresi + 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
14-Sendika üyeliği, Sendika üyeliği bilgileri vb.	Çalışma süresi sona erinceye kadar	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
15-Sağlık bilgileri, engellilik durumuna ait bilgiler, kan grubu bilgisi, kişisel sağlık bilgileri, kullanılan cihaz ve protez bilgileri vb.	100 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
16-Ceza mahkûmiyeti ve güvenlik tedbirleri, Ceza mahkumiyetine ilişkin bilgiler, güvenlik tedbirlerine ilişkin bilgiler vb.	15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
17-Biyometrik veri, Avuç içi bilgileri, parmak izi bilgileri, retina taraması bilgileri, yüz tanıma bilgileri vb.	Akademik çalışmalarda işlenen veriler anonimleştirilerek saklanmaktadır	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
18-Genetik veri, Genetik veriler vb.	Akademik çalışmalarda işlenen veriler anonimleştirilerek saklanmaktadır	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
19-Toplantı vb. etkinlik katılımcılarına ait görsel ve işitsel kayıtlar	Etkinliğin sona ermesini takiben 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
20-Kadro başvurusu kabul edilmediği takdirde aday başvurularına ilişkin veriler	Yükseköğretim Üst Kuruluşları ve Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planında öngörülen süreler	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
21-Staj başvurusu kabul edilmediği takdirde aday başvurularına ilişkin veriler	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
22-Memnuniyet anketi katılımcıları	Anketin sona ermesini takip	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

	eden 1 ay içerisinde	
23-Sözleşmelerin hazırlanması ve işlenmesine ilişkin veriler	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

11- KİŞİSEL VERİLERİN PERİODİK İMHA SÜRELERİ

Yönetmeliğin 11 inci maddesi gereğince periyodik imha süresi 6 ay olarak belirlemiştir. Buna göre, tüm kişisel veriler için 6 aylık zaman aralıklarında (Her yılın Ocak ve Temmuz aylarının sonunda) ilgili birimler tarafından periyodik imha gerçekleştirilir.

12- POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Kişisel Verilerin Korunması Birimi dosyasında saklanır.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınmakta ve bu kayıtlar diğer hukuki yükümlülükler hariç olmak kaydıyla en az üç yıl süre ile saklanmaktadır.

13- POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

14- POLİTİKA'NIN YÜRÜRLÜĞÜ *VE YÜRÜRLÜKTEN KALDIRILMASI*

Politika, Üniversite Yönetim Kurulu tarafından kabul edilmesini müteakiben Üniversitenin internet sitesinde yayınlanması ile yürürlüğe girmiş kabul edilir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshası Üniversite Yönetim Kurulu Kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Kişisel Verilerin Korunması Birimi tarafından saklanır.