1. **AMAÇ:**

Bu politikanın amacı, Yıldız Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı personellerine ait tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin önlemleri belirlenmelidir.

1. **KAPSAM:**

Bu politika; 6698 sayılı Kanunun 7 nci maddesinin üçüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Ki̇şi̇sel Veri̇leri̇n Si̇li̇nmesi̇, Yok Edi̇lmesi̇ Veya Anoni̇m Hale Geti̇ri̇lmesi̇ Yönetmeliğine uygun olarak hazırlanmıştır.

1. **TANIMLAR**

**Alıcı grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

**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 kişileridir

**İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

**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 ifade eder.

**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 envanterdir.

**Kişisel veri saklama ve imha politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

**Periyodik imha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini ifade eder.

**Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.

**Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

**Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

**Kişisel verilerin silinmesi** Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

**Kişisel verilerin yok edilmesi** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

**Kişisel verilerin anonim hale getirilmesi**Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve 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 getirilmesi gerekir.

1. **KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI İLE DÜZENLENEN KAYIT ORTAMLARI** 
   1. Kağıt ortamlar
      1. Kağıt
      2. Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)
      3. Yazılı, basılı, görsel ortamlar
   2. Elektronik ortamlar
      1. Sunucular (Etki alanı, yedekleme, e-posta,
      2. veritabanı, web, dosya paylaşım, vb.)
      3. Yazılımlar
      4. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb. )
      5. Kişisel bilgisayarlar (Masaüstü, dizüstü)
      6. Mobil cihazlar (telefon, tablet vb.)
      7. Optik diskler (CD, DVD vb.)
      8. Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
      9. Yazıcı, tarayıcı, fotokopi makinesi
2. **SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER**

* 6698 sayılı Kişisel Verilerin Korunması Kanunu,
* 6098 sayılı Türk Borçlar Kanunu,
* 4734 sayılı Kamu İhale Kanunu,
* 657 sayılı Devlet Memurları Kanunu,
* 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
* 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar
* Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
* 5018 sayılı Kamu Mali Yönetimi Kanunu,
* 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
* 4982 Sayılı Bilgi Edinme Kanunu,
* 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun
* 4857 sayılı İş Kanunu,
* 2547 sayılı Yükseköğretim Kanunu,
* 5434 sayılı Emekli Sağlığı Kanunu,
* 2828 sayılı Sosyal Hizmetler Kanunu
* İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
* Arşiv Hizmetleri Hakkında Yönetmelik
* Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

1. **SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI**

* Acil Durum Yönetimi Süreçlerinin Yürütülmesi
* Bilgi Güvenliği Süreçlerinin Yürütülmesi
* Çalışan Adayı / Stajyer / Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi
* Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
* Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi
* Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
* Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
* Denetim / Etik Faaliyetlerinin Yürütülmesi
* Eğitim Faaliyetlerinin Yürütülmesi
* Erişim Yetkilerinin Yürütülmesi
* Faaliyetlerin Mevzuata Uygun Yürütülmesi
* Finans ve Muhasebe İşlerinin Yürütülmesi
* Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
* Fiziksel Mekan Güvenliğinin Temini
* Görevlendirme Süreçlerinin Yürütülmesi
* Hukuk İşlerinin Takibi Ve Yürütülmesi
* İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
* İletişim Faaliyetlerinin Yürütülmesi
* İnsan Kaynakları Süreçlerinin Planlanması
* İş Faaliyetlerinin Yürütülmesi / Denetimi
* İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
* İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
* İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
* Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
* Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
* Mal / Hizmet Satış Süreçlerinin Yürütülmesi
* Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
* Organizasyon ve Etkinlik Yönetimi
* Performans Değerlendirme Süreçlerinin Yürütülmesi
* Risk Yönetimi Süreçlerinin Yürütülmesi
* Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
* Sosyal Sorumluluk ve Sivil Toplum Aktivitelerinin Yürütülmesi
* Sözleşme Süreçlerinin Yürütülmesi
* Sponsorluk Faaliyetlerinin Yürütülmesi
* Stratejik Planlama Faaliyetlerinin Yürütülmesi
* Talep / Şikayetlerin Takibi
* Taşınır Mal ve Kaynakların Güvenliğinin Temini
* Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
* Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
* Yönetim Faaliyetlerinin Yürütülmesi
* Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

1. **İMHAYI GEREKTİREN SEBEPLER**

* Kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.
* Türk Ceza Kanunu’nun 138. maddesinde ve KVK Kanunu’nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Üniversite kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir.
* İlgili kişi, Üniversiteye başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.
* Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Üniversite talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Üniversite, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.
* Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Üniversite bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.
* Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Üniversite tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

**Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler**

* Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
* Ağ yoluyla veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
* Anahtar yönetimi uygulanmaktadır.
* Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
* Çalışanlar için yetki ve yetki devri ilgili dokümanlarca oluşturulmuştur.
* Erişim logları düzenli olarak tutulmaktadır.
* Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
* Gerektiğinde veri maskeleme yöntemi uygulanmaktadır.
* Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
* 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 veri içeren ortamların güvenliği sağlanmaktadır.
* Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
* Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de 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 işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
* Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
* Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
* Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
* Gizlilik taahhütnameleri yapılmaktadır.
* İmzalanan taahhütnameler veri güvenliği hükümleri içermektedir.
* Kişisel veri güvenliğine yönelik dokümantasyon hazırlanmıştır.
* Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
* Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
* Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler mevcuttur.

**Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler**

* Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılır ve kayıt altına alınır.
* Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

**Ki̇şi̇sel Veri̇leri̇n Si̇li̇nmesi̇, Yok Edi̇lmesi̇ ve Anoni̇mleşti̇ri̇lmesi̇ Tekni̇kleri̇**

* **Fiziksel Olarak Yok Etme**  Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Örnek: İlgili dosyanın, belgenin kağıt kırpma makinesi ile imhası.
* **Yazılımdan Güvenli Olarak Silme**  Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; çok yüksek ihtimalle bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.
* **Uzman Tarafından Güvenli Olarak Silme**Üniversite bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.
* **Kişisel Verileri Anonim Hale Getirme Teknikleri**
* Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Üniversite, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.
* KVK Kanunu’nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.
* **Maskeleme (Masking)**Veri maskeleme, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.  Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, TC Kimlik No, ad, soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkansız hale geldiği bir veri setine dönüştürülmesi.
* **Toplulaştırma (Aggregation)**Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.  Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.
* **Veri Türetme (Data Derivation)** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır.   Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehirin belirtilmesi.
* **Veri Karma (Data Shuffling, Permutation)**  Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır.   Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

**Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimleri ve görev tanımları:**

* *Bilgi İşlem Daire Başkanlığı;* Üniversite’nin tüm Bilgi İşlem süreçlerini yönetir.
* *Hukuk İşleri Daire Başkanlığı,* Üniversite’nin tüm hukuki işlem süreçlerini yönetir.
* *Personel Daire Başkanlığı; (Personel ile ilgili konularda)*, Üniversite’nin tüm personel süreçlerini yönetir.
* *Öğrenci işleri Daire Başkanlığı;* (Öğrenclerle ilgili konularda) Üniversite’nin tüm öğrenci süreçlerini yürütür.
* *İletişim Koordinatörlüğü*Üniversitesinin kendi içinde yaptığı her türlü yazışmanın, web sayfasında ve diğer dijital mecralarda ki tanıtımının organize edilmesi, takip edilmesi ve işler konumda tutulmasını sağlarken, kendi içindeki bütün birimlerle koordineli olarak çalışmaktadır. Gerek akademik gerekse idari anlamda yürütülen her türlü faaliyetin düzenli ve kurallı uygulanışından, haber, bilgi, tanıtım materyali, afiş, grafik pop-up uygulamaları, yazılı ve görsel basının takip edilmesi, arşivleme, tasnif etme ve düzenli olarak yıllık yayınlama gibi işleri yürütür.

1. **SAKLAMA VE İMHA SÜRELERİNİ GÖSTEREN TABLO**

|  |  |  |
| --- | --- | --- |
| **NO** | **VERİ KATEGORİSİ** | **VERİ SAKLAMA SÜRESİ** |
| **1** | **Kimlik** | **101 YIL** |
| **2** | **İletişim** | **101 YIL** |
| **3** | **Lokasyon** | **2 YIL** |
| **4** | **Özlük** | **101 YIL** |
| **5** | **Hukuki İşlem** | **10 YIL** |
| **6** | **Müşteri İşlem** | **101 YIL** |
| **7** | **Fiziksel Mekân Güvenliği** | **2 YIL** |
| **8** | **İşlem Güvenliği** | **2 YIL** |
| **9** | **Risk Yönetimi** | **10 YIL** |
| **10** | **Finans** | **10 YIL** |
| **11** | **Mesleki Deneyim** | **101 YIL** |
| **13** | **Görsel ve İşitsel Kayıtlar** | **101 YIL** |
| **18** | **Sendika Üyeliği** | **101 YIL** |
| **18** | **Sağlık Bilgileri** | **101 YIL** |
| **19** | **Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri** | **101 YIL** |

**\*Yukarıdaki süreler, çalışanlar için iş sözleşmesinin feshi tarihinden, öğrenciler için Üniversite ile ilişiğin kesildiği tarihten, tedarikçiler için sözleşmenin sona erme tarihinden veya sözleşme yoksa son işlemin yapıldığı tarihten, diğer ilgili kişiler için kişisel verilerin elde edilme tarihinden itibaren başlar.**

1. **PERİYODİK İMHA SÜRELERİ**

* Üniversite saklama süresi dolan kişisel verileri saklama süresinin dolduğu tarihten itibaren en geç 180 gün içerisinde imha eder.
* Üniversite; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.
* Periyodik imhanın gerçekleştirileceği zaman aralığı veri sorumlusu tarafından kişisel veri saklama ve imha politikasına, prosedürlere ve Üniversite’nin iş akışına uygun olarak belirlenir. Bu süre her halde altı ayı geçemez.

1. **YAPTIRIM**

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır.