1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kişisel verilerin işlenmesi, korunması, saklanması, aktarılması, erişilmesi ve gerektiğinde imha edilmesine ilişkin süreçlerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat doğrultusunda yürütülmesini sağlamaktır.

Bu prosedür ile kişisel veri işleme faaliyetlerinin hukuka uygun şekilde gerçekleştirilmesi, ilgili kişilerin haklarının korunması, kişisel veri güvenliğine ilişkin idari ve teknik tedbirlerin uygulanması ve kişisel veri işleme süreçlerinin izlenebilir şekilde yönetilmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür, Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde gerçekleştirilen kişisel veri işleme faaliyetlerini ve bu faaliyetlerde görev alan çalışanları, ilgili kişileri, veri işleyenleri ve yetkilendirilmiş üçüncü tarafları kapsar.

3. TANIMLAR

- **Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- **Özel Nitelikli Kişisel Veri:** 6698 sayılı Kanun kapsamında özel nitelikte kabul edilen kişisel verileri,
- **İlgili Kişi:** Kişisel verisi işlenen gerçek kişiyi,
- **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişiyi,
- **Veri İşleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- **Kişisel Veri İşleme Envanteri:** Veri sorumlularının işleme faaliyetlerine ilişkin olarak oluşturduğu ve kişisel veri işleme süreçlerine ilişkin bilgileri içeren kayıtları,
- **Kişisel Veri İhlali:** Kişisel verilerin hukuka aykırı olarak elde edilmesi, açıklanması, değiştirilmesi, kaybolması veya erişilemez hale gelmesi gibi kişisel veri güvenliğini etkileyen olayları,
- **KVKK:** 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- **EYS:** Süleyman Demirel Üniversitesi Entegre Yönetim Sistemini ifade eder.
- **Aydınlatma:** Kişisel verilerin işlenmesi hakkında ilgili kişilerin mevzuatta öngörülen hususlarda bilgilendirilmesini,
- **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı,

4. SORUMLULUKLAR

- **Üst Yönetim:** Kişisel verilerin korunmasına yönelik gerekli kaynak ve organizasyonun sağlanmasını desteklemek.
- **KVKK Komisyonu / Yetkili Birim:** Kişisel veri süreçlerinin mevzuata uygun yürütülmesini koordine etmek ve gerekli değerlendirmeleri yapmak.

- **Birim Yöneticileri:** Birimlerindeki kişisel veri işleme faaliyetlerinin kurallara uygun yürütülmesini ve envanter bilgilerinin güncel tutulmasını sağlamak.
- **Bilgi İşlem Daire Başkanlığı:** Kişisel veri güvenliğine yönelik teknik tedbirlerin ve bilgi sistemleri üzerindeki güvenlik kontrollerinin uygulanmasını sağlamak.
- **Çalışanlar:** Görevleri kapsamında eriştikleri kişisel verileri yalnızca yetkileri doğrultusunda işlemek, korumak ve gizlilik kurallarına uymak.
- **Veri İşleyenler ve Üçüncü Taraflar:** Üniversite tarafından belirlenen kişisel veri güvenliği şartlarına ve ilgili mevzuata uygun hareket etmek.

5. UYGULAMA

5.1. Kişisel Veri İşleme Faaliyetlerinin Yönetimi

Kişisel veriler yalnızca belirli, açık ve meşru amaçlar doğrultusunda ve ilgili mevzuatta belirtilen işleme şartlarına dayanılarak işlenir.

Kişisel veri işleme faaliyetlerinde;

- Hukuka ve dürüstlük kurallarına uygunluk,
- Doğruluk ve gerektiğinde güncellik,
- Belirli, açık ve meşru amaçlarla işleme,
- İşleme amacıyla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işleme amacı için gerekli süre kadar muhafaza etme ilkelerine uyulur.

Birimlerde yeni bir kişisel veri işleme faaliyeti başlatılmadan önce işleme amacı, veri kategorileri, ilgili kişi grubu, hukuki dayanak, aktarım ihtiyacı, saklama süresi ve uygulanacak güvenlik tedbirleri değerlendirilir.

5.2. Kişisel Veri İşleme Envanteri

Üniversitede gerçekleştirilen kişisel veri işleme faaliyetleri ilgili envanter kayıtlarında tanımlanır. Birimler, sorumlu oldukları kişisel veri işleme faaliyetlerine ilişkin bilgilerin güncel ve doğru tutulmasını sağlar. Aşağıdaki durumlarda ilgili envanter kayıtları gözden geçirilir ve gerekli güncellemeler yapılır:

- Yeni bir kişisel veri işleme faaliyeti başlatılması,
- Mevcut işleme faaliyetinin amacının veya kapsamının değişmesi,
- Yeni kişisel veri kategorilerinin işlenmesi,
- İlgili kişi gruplarının değişmesi,
- Yeni aktarım yapılan tarafların ortaya çıkması,
- Saklama sürelerinin değişmesi,
- Yeni bilgi sistemi veya uygulamanın kullanılmaya başlanması,
- Kişisel veri işleme faaliyetini etkileyen mevzuat veya süreç değişiklikleri.
-

5.3. Kişisel Veri İşleme Şartlarının Değerlendirilmesi

Kişisel veriler, 6698 sayılı Kanunda belirtilen işleme şartlarından en az birine dayanılarak işlenir. Özel nitelikli kişisel verilerin işlenmesinde Kanunun güncel hükümleri ve Kişisel Verileri Koruma Kurulu tarafından belirlenen şart ve tedbirler dikkate alınır. 2024 yılında yapılan değişikliklerle özel nitelikli kişisel verilerin işlenmesine ilişkin hukuki sebepler genişletildiğinden, bu veriler için her durumda açık rıza alınması yoluna gidilmez; öncelikle uygulanabilir hukuki dayanak değerlendirilir.

Kişisel veri işleme şartının veya işleme amacının ortadan kalkması halinde veriler, mevzuat ve Üniversitenin saklama ve imha kurallarına uygun olarak silinir, yok edilir veya anonim hale getirilir.

5.4. Aydınlatma Yükümlülüğü

Kişisel verileri işlenen ilgili kişilerin, 6698 sayılı Kanun kapsamında gerekli bilgilendirmeleri alması sağlanır.

Aydınlatma metinlerinde gerekli durumlarda;

- Veri sorumlusunun kimliği,
- Kişisel verilerin hangi amaçla işlendiği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- İlgili kişinin hakları hakkında bilgi verilir.

Kişisel veri işleme faaliyetinin niteliğine göre ilgili kişilere uygun yöntemle aydınlatma yapılır.

Aydınlatma metinleri;

- İlgili birimlerde fiziksel olarak erişilebilir şekilde,
- Üniversitenin internet sitesi veya ilgili elektronik ortamlarında,
- Gerektiğinde QR kod veya benzeri erişim yöntemleri kullanılarak ilgili kişilerin erişimine sunulabilir.

Aydınlatma yükümlülüğünün yerine getirilmesi, kural olarak ilgili kişinin ayrıca imza vermesine veya açık rıza göstermesine bağlanmaz.

5.5. Açık Rıza Gerektiren İşleme Faaliyetleri

Kişisel veri işleme faaliyetinin hukuki dayanağının açık rıza olması gereken durumlarda, açık rızanın belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle verilmesi sağlanır.

Açık rıza alınması gereken durumlarda;

- Açık rıza metni ilgili işleme faaliyetinden ayrı olarak düzenlenir,
- Hangi kişisel verilerin hangi amaçla işleneceği açıkça belirtilir,
- Açık rıza vermemenin sonuçları hukuka uygun ve anlaşılır şekilde açıklanır,
- Açık rıza kayıtları gerektiğinde gösterilebilecek şekilde muhafaza edilir.

Açık rıza alınması gereken bir faaliyette ilgili kişinin rıza vermemesi halinde, mevzuata aykırı şekilde hizmetin engellenmesi veya rıza vermeye zorlanması yoluna gidilmez.

5.6. İlgili Kişi Başvuruları

İlgili kişilerin 6698 sayılı Kanunun 11'inci maddesinde belirtilen haklarını kullanmak amacıyla yapacakları başvurular, Üniversite tarafından belirlenen başvuru usul ve esasları doğrultusunda alınır ve değerlendirilir. Başvuruların mevzuatta belirtilen süreler içerisinde sonuçlandırılması sağlanır. Başvuruların değerlendirilmesi sırasında gerektiğinde ilgili birimlerden bilgi ve belge alınır. Birimlere doğrudan ulaşan kişisel veri talepleri, Üniversite tarafından belirlenen yetkili başvuru sürecine yönlendirilir ve gerekli kayıtların oluşturulması sağlanır.

5.7. Kişisel Verilerin Aktarılması

Kişisel verilerin yurt içi veya yurt dışına aktarılması, 6698 sayılı Kanun ve ilgili mevzuatta belirtilen şartlar doğrultusunda gerçekleştirilir.

Veri aktarımı yapılmadan önce;

- Aktarım amacı,
- Aktarılacak veri kategorileri,
- Aktarım yapılacak taraf,
- Aktarımın hukuki dayanağı,
- Aktarımın güvenlik koşulları değerlendirilir.

Yurt dışına veri aktarımında Kanunun güncel hükümleri kapsamında öngörülen yeterlilik kararı, uygun güvenceler veya uygulanabilir istisnai şartlar dikkate alınır.

Veri işleyen veya üçüncü taraflarla gerçekleştirilen veri aktarım süreçlerinde gerekli sözleşme, taahhüt ve güvenlik şartları uygulanır.

5.8. Kişisel Veri Güvenliğinin Sağlanması

Kişisel verilerin güvenliğinin sağlanması amacıyla uygun idari ve teknik tedbirler uygulanır. Teknik tedbirler kapsamında, bilgi sistemlerinin niteliğine ve risklere göre;

- Erişim yetkilendirmeleri,
- Kullanıcı kimlik doğrulama kontrolleri,
- Ağ ve sistem güvenliği,
- Kötücül yazılımlara karşı koruma,
- Güncelleme ve yama yönetimi,
- Loglama ve izleme,
- Yedekleme,
- Veri aktarım güvenliği,
- Güvenlik açıklıklarının giderilmesi gibi kontroller uygulanır.

İdari tedbirler kapsamında ise kişisel veri güvenliği konusunda çalışanların farkındalığının artırılması, görev ve sorumlulukların belirlenmesi, gizlilik yükümlülükleri ve gerekli politika/prosedürlerin uygulanması sağlanır.

5.9. Erişim Yetkilerinin Yönetimi

Kişisel verilere erişim, görev ve sorumluluklar doğrultusunda yetkilendirilir.

Kullanıcıların yalnızca görevlerini yerine getirmek için ihtiyaç duydukları kişisel verilere erişebilmesi sağlanır. Personelin;

- Göreve başlaması,
- Görev veya birim değiştirmesi,
- Yetkisinin değişmesi,
- Görevden ayrılması durumlarında kişisel verilere ilişkin erişim yetkileri gözden geçirilir ve gerekli değişiklikler zamanında gerçekleştirilir.

5.10. Personel görev Değişikliği ve Görevden Ayrılma

Personelin görev veya birim değişikliği halinde mevcut kişisel veri erişimleri ve yetkileri yeni görevine göre değerlendirilir. Görevden ayrılan personelin kişisel verilere ve kişisel veri içeren bilgi sistemlerine erişim yetkileri kaldırılır. Personele teslim edilmiş kişisel veri içeren fiziksel veya elektronik ortamlar, bilgi sistemleri, cihazlar, dokümanlar ve diğer kurumsal varlıklar ilgili süreçlere uygun olarak iade alınır veya erişimleri sonlandırılır.

5.11. Kişisel Veri İhlallerinin Yönetimi

Kişisel veri güvenliğini etkileyebilecek ihlal veya şüpheli durumlar gecikmeksizin ilgili birimlere bildirilir. İhlal tespit edilmesi halinde;

- Olayın kapsamı,
- Etkilenen kişisel veri kategorileri,
- Etkilenen ilgili kişi grupları,
- Olası riskler,
- İhlalin kaynağı,
- Alınabilecek düzeltici ve önleyici tedbirler değerlendirilir.

Gerekli teknik ve idari tedbirler uygulanır. Mevzuat kapsamında Kurula veya ilgili kişilere bildirim yapılmasının gerekli olduğu durumlarda yetkili süreç işletilir. İhlale ilişkin kayıtlar ve kanıtlar, olay ve ihlal yönetimi süreçlerine uygun şekilde muhafaza edilir.

5.12. Özel Nitelikli Kişisel Verilerin Korunması

Özel nitelikli kişisel verilerin işlenmesi sırasında Kanunda öngörülen işleme şartları ve Kurul tarafından belirlenen yeterli önlemler dikkate alınır. Bu verilerin bulunduğu fiziksel ve elektronik ortamlara erişim görev gerekliliği ile sınırlandırılır.

Özel nitelikli kişisel verilerin;

- Fiziksel olarak saklanması,
- Elektronik ortamda tutulması,
- Kurum içi veya dışı aktarılması,
- Yedeklenmesi,
- İmha edilmesi süreçlerinde risklere uygun teknik ve idari tedbirler uygulanır.

5.13. Temiz Masa ve Temiz Ekran Uygulamaları

- Kişisel veri içeren basılı dokümanlar, dosyalar, formlar ve benzeri materyaller yetkisiz kişilerin erişimine açık bırakılmaz.
- Çalışanlar görevleri sona erdiğinde kişisel veri içeren dokümanları güvenli şekilde muhafaza eder.
- Bilgisayar ve diğer bilgi sistemlerinde kişisel verilerin yetkisiz kişilerce görülmesini önlemek amacıyla ekran kilitleme ve benzeri güvenlik önlemleri kullanılır.
- Kişisel veri içeren dokümanların ortak alanlarda, yazıcılarda, toplantı salonlarında veya çalışma alanlarında kontrolsüz şekilde bırakılmasına izin verilmez.

5.14. Kişisel Veri içeren Dokümanların fiziksel Güvenliği

Kişisel veri içeren fiziksel dokümanlar, görev gereği erişim yetkisi bulunan kişiler dışında erişilemeyecek şekilde muhafaza edilir. Kişisel veri içeren dokümanların kopyalanması, çoğaltılması, paylaşılması ve taşınması sırasında veri güvenliği gözetilir. İmha edilmesi gereken fiziksel dokümanlar, Üniversitenin saklama ve imha süreçlerine uygun olarak imha edilir.

5.15. Saklama ve İmha

Kişisel veriler, ilgili mevzuatta öngörülen veya işleme amacı için gerekli olan süre kadar muhafaza edilir. Saklama süresinin sona ermesi veya işleme amacının ortadan kalkması halinde kişisel veriler, Üniversitenin kişisel veri saklama ve imha kurallarına uygun olarak silinir, yok edilir veya anonim hale getirilir. İmha işlemleri kayıt altına alınır.

5.16. Farkındalık ve Eğitim

Kişisel verilerin korunması konusunda görev ve sorumlulukları bulunan çalışanlara yönelik gerekli farkındalık ve eğitim faaliyetleri gerçekleştirilir. Eğitim ve farkındalık faaliyetlerinin içeriği görev, yetki ve kişisel veri işleme faaliyetlerinin niteliğine göre belirlenir.

5.17. Tedarikçi ve Üçüncü Taraflarla Çalışmalar

Kişisel veri işlenmesini gerektiren mal veya hizmet alımlarında, ilgili tarafın kişisel veri işleme faaliyetleri değerlendirilir. Veri işleyenler ve üçüncü taraflarla yapılan sözleşmelerde, hizmetin niteliğine uygun kişisel veri güvenliği, gizlilik, erişim, aktarım, saklama, ihlal bildirimi ve imha yükümlülüklerine yer verilmesi sağlanır. Tedarikçi veya üçüncü tarafın kişisel verilere erişimi, ihtiyaç ve yetki ile sınırlandırılır.

5.18. Yeni Sistem, Uygulama ve Süreçlerde Kişisel Verilerin Korunması

Yeni bir bilgi sistemi, uygulama, hizmet veya iş süreci oluşturulurken kişisel veri işlenip işlenmediği değerlendirilir. Kişisel veri işlenmesi halinde;

- İşleme amacı,
- İşlenecek veri kategorileri,
- İlgili kişi grupları,
- Hukuki dayanak,
- Saklama süresi,
- Aktarım ihtiyacı,
- Erişim yetkileri,
- Teknik ve idari güvenlik tedbirleri değerlendirilerek gerekli kayıt ve kontroller oluşturulur. Gereksiz kişisel veri toplanmasından ve işlenmesinden kaçınılır.

5.19. Kişisel Veri İşleme Faaliyetlerinin Gözdem Geçirilmesi

Kişisel veri işleme faaliyetleri;

- Mevzuat değişiklikleri,
- Yeni iş süreçleri,
- Yeni bilgi sistemleri,
- Yeni veya değişen riskler,
- Organizasyonel değişiklikler,
- Kişisel veri ihlalleri,
- Denetim ve kontrol sonuçları dikkate alınarak gerektiğinde gözden geçirilir.

Tespit edilen uygunsuzluk, risk veya iyileştirme ihtiyacı için Üniversitenin düzeltici ve iyileştirici faaliyet süreçleri işletilir.

5.20. Kontrol ve Değerlendirme Faaliyetleri

Kişisel verilerin korunmasına ilişkin birim uygulamaları, yapılan kontroller ve değerlendirmeler kapsamında gözden geçirilebilir.

KVKNET ONE E-Danışman modülü üzerinden veya benzeri kontrol ve değerlendirme araçlarından elde edilen sonuçlar, gerekli görüldüğünde;

- Uygunsuzluk,
- Risk,
- Düzeltici faaliyet,
- İyileştirme faaliyeti,
- Eğitim ve farkındalık ihtiyacı,
- Teknik veya idari tedbir ihtiyacı olarak değerlendirilir.

5.21. Disiplin ve Uygunsuzluklar

Kişisel verilerin bu prosedür, ilgili politika ve diğer EYS dokümanlarına veya mevzuata aykırı şekilde işlenmesi, açıklanması, aktarılması, yetkisiz kişilerin erişimine sunulması veya güvenlik tedbirlerinin ihlal edilmesi durumunda olayın niteliğine göre gerekli idari ve disiplin süreçleri uygulanır.

Tespit edilen uygunsuzluklar için gerektiğinde düzeltici ve iyileştirici faaliyet başlatılır.

6. İLGİLİ DOKÜMANLAR

- Kişisel Veri Envanter Listesi
- Aydınlatma Metinleri
- İlgili Kişi Başvuru Formu
- Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası
- Kişisel Veri Saklama ve İmha Prosedürü
- Olay ve İhlal Yönetimi ile ilgili EYS dokümanları
- Birim Hassas Veri Dosyası Dolap Açma Kapama Takip Formu

7.REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	06.12.2024	İlk yayın.
001	16.09.2026	SDÜ EYS yapısına uyum sağlanması; kapsam, sorumluluklar ve kişisel veri işleme, envanter, aydınlatma, açık rıza, ilgili kişi başvuruları, veri aktarımı, özel nitelikli kişisel veriler, veri güvenliği, erişim, ihlal, personel değişiklikleri, fiziksel güvenlik, eğitim, tedarikçi yönetimi, saklama-imha ve kontrol süreçlerinin güncellenmesi.