

T.C.

NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

1. Amaç

Bu politikanın amacı;

- Niğde Ömer Halisdemir Üniversitesi (Üniversite) tarafından yürütülen her türlü faaliyette 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) uygun olarak kişisel veri işleme faaliyeti ve kişisel verilerin korunmasına yönelik benimsenen yöntemleri tarif etmek,
- Üniversitenin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve üçüncü kişiler olmak üzere Üniversite tarafından işlenen tüm kişisel verileri, Üniversitenin kişisel verilerin korunmasına yönelik benimsemiş olduğu ilkeler ve kurmuş olduğu sistemler konusunda bilgilendirerek şeffaflığı sağlamaktır.

2. Kapsam ve Dayanak

Üniversitenin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve üçüncü kişiler olmak üzere kişisel verileri Üniversite tarafından işlenen tüm kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla Üniversitenin süreçlerinde işlenen tüm kişisel verileri kapsar.

Bu politika 7/4/2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'na ve ilgili diğer yasal düzenlemelere dayanılarak hazırlanmıştır.

3. Yetki ve Sorumluluklar

Üniversite içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verilerin saklanması, korunması, işlenmesi ve imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, dış hizmet sağlayıcıları ve diğer surette Üniversite nezdinde kişisel veri saklayan ve işleyen herkes sorumludur. Her birim kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür. İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak imhalara; ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri işlemeyi yapan iş birimi dikkate alınarak Rektörlükçe belirlenen ilgili komisyon karar verecektir. Kişisel Verileri Koruma Kurumu ile yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme ve sicile kayıt gibi işlemlerin sorumluluğu veri sorumlusu irtibat kişisindedir.

4. Tanımlar ve Kısaltmalar

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

İlgili/Yetkili 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 kişilerdir.

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

Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

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 ortam.

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

Üniversite: Niğde Ömer Halisdemir Üniversitesi

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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.

Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili/yetkili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.

Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.

Kurul: Kişisel Verileri Koruma Kurulu.

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.

Veri Sahibi/İlgili Kişi; Kişisel verisi işlenen gerçek kişi.

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

Yönetmelik: 28 /10/2017 tarihli ve 30224 sayılı Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

5. Kişisel Verilerin Korunması ve İşlenmesi Politikası

Üniversite kişisel verilerin korunması ve işlenmesi için gerekli tedbirleri ve uygulanan süreci politika ile somut bir şekilde belirler. İlgili kanunlar ve yönetmelikler ile bu politikanın uyumsuz olduğu durumlarda ya da güncellenen mevzuatlar doğrultusunda politikanın güncel olmaması halinde Üniversite yürürlükteki mevzuata uyacağını kabul eder. Yasal düzenlemelerdeki değişikliklere göre bu politika güncellenir.

5.1. Kişisel Verilerin Güvenliğinin Sağlanması

Üniversite, KVKK'nın 12 inci maddesinin 1inci fıkrasında öngörülen;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak,

için gerekli her türlü teknik ve idari tedbirleri alır.

Üniversitenin kişisel verilerin güvenliğini sağlamak için uyguladığı tedbirler alt maddelerde detaylandırılmıştır.

5.1.1.İdari Tedbirler

Üniversite veri güvenliğini sağlamak amacıyla bilgili ve deneyimli kişiler istihdam eder ve personeline gerekli bilgi güvenliği farkındalığı ve kişisel verileri koruma ile ilgili eğitimleri verir. Kişisel verilerin güvenliğini sağlamak amacı ile gerekli idari tedbirleri alır ve çalışanların bu tedbirlere göre çalışmalarını denetler. İş birim bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak ve iş süreçlerinin aksamasına neden olmayacak düzeyde erişim ve yetkilendirmeleri tanımlar. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerini ve kurallarını tanımlar. Çalışanlar, öğrendikleri kişisel verileri KVKK'nın hükümlerine aykırı olarak başkasına açıklayamayacağı, işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılımlarından sonra da devam edeceği konusunda bilgilendirilir. Çalışanlardan bu doğrultuda gerekli taahhütler alınır. Üçüncü taraflarla kişisel verilerin paylaşılmasıyla ilgili olarak kişisel verilerin paylaşıldığı kişilerle çerçeve sözleşme imzalanır yahut sözleşmelere ekleyeceği hükümler ile veri güvenliğini sağlar. Kişisel veri

paylaşılan üçüncü taraflar kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümleri kabul eder. Alınan önlemlere rağmen işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiği tespit edilmesi halinde veri sorumlusu irtibat kişisi tarafından ilgisine ve KVK Kuruluna bildirir. Kişisel verinin nasıl başkaları tarafından elde edildiği araştırılır. Üniversite tespit ettiği zafiyeti gidermek için gerekli idari tedbirleri uygular, ihtiyaç halinde teknik tedbirler alır.

5.1.2. Teknik Tedbirler

Üniversite, kurulan sistemler için gerekli iç kontrolleri yapar. Kurulan sistemler kapsamında risk analizi, veri sınıflandırması, bilgi güvenliği risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini işletir. Bu süreçler doğrultusunda teknolojiye gelişmelere uygun teknik önlemleri alır. Gelişen teknolojiye uygun altyapı yatırımları yapar. Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımların kurulmasını sağlar. Sistemlerinin güncel ve bilinen açıklıklara karşı gerekli güvenlik önlemlerinin alınmış versiyonlarını kullanır. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişimi yetkilerinin kontrol altında tutulmasını sağlar. Üniversitede işlenmekte olan kişisel verilerin saklandığı fiziki alanlar, çalınmaya ve kaybolmaya karşı gerekli fiziksel güvenlik önlemleri alınarak muhafaza edilir. Aynı şekilde kişisel verilerin yer aldığı ortamlar dış risklere (yangın, sel, deprem vb.) karşı gerekli uygun yöntemler belirlenerek koruma altına alınır. Bu ortamlara giriş çıkışlar kayıt altına alınarak izlenir. Kişisel veri barındıran sunucular Üniversite sistem odasında muhafaza edilir. Sistem odasının fiziki güvenlik önlemleri alınır. Kişisel veri barındıran sistem, uygulama, veri tabanı vb. alanlara erişim için kullanılmakta olan şifreler, karmaşık bir algoritma ile üretilir ve sistemler bu şekilde kullanılmaya teşvik edilir. İş birim bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak erişim ve yetkilendirme tanımlarını yapar. Erişimlerin yetkilendirmelere uygunluğunu kontrol eder. Risk teşkil eden noktalar tespit edilerek gerekli teknik tedbirler alınır. Kişisel verilerin güvenliğinin sürdürülebilmesi için teknik tedbirleri sürekli işleyen bir model ile kurum kültürünün bir parçası olması için farkındalığı yaygınlaştırır.

Birimlerce takip edilen kamera kayıtları ilgili birimlerde yer alır, kamera kayıtlarına erişimde kullanıcı yetkilendirilmesi yapılır ve veriler güvenli ortamda saklanır.

5.1.3. Kişisel Verilerin Korunmasının Sürdürülebilirliği İçin Yapılan Denetimler

Üniversite, KVKK'nın 12 inci maddesine uygun olarak, gerekli denetimleri yapar ve yaptırır. Bilgi Güvenliği Yönetim Sistemi ve Veri Koruma Kişisel Bilgi Yönetimi sistemlerinin sürdürülebilirliğini sağlamak için iç ve dış denetimlerin yapılmasını sağlar. Sistemlerde oluşabilecek teknik açıklıklar için düzenli olarak sistemlere sızma testlerini gerçekleştirir. Bilgi işlem tarafından sistemler düzenli olarak izlenir. Ayrıca siber saldırılara karşı güvenliğin sağlanması için sistem iz kayıtları takip edilir. Yönetim sistemleri ve uyarı sistemlerinin ürettiği veriler ve sistemlerin izlenmesi ile tespit edilen bulgular için gerekli teknik ve idari tedbirler alınır.

5.1.4. Kişisel Verilerin Yetkisiz İfşası Durumunda Alınan Tedbirler

Üniversite, KVKK'nın 12 inci maddesine uygun olarak işlenen kişisel verilerin yetkisiz ifşa olması halinde ilgili kişisel veri sahibine ve KVK Kurulu'na bilgi verir. KVK Kurulu tarafından gerek görülmesi halinde, bu durum, KVK Kurulu'nun internet sitesinde veya başka bir yöntemle ilan edilebilir.

5.1.5. Üçüncü Tarafların Kişisel Verilerin Korunmasını Sağlaması İçin Uygulanan Tedbirler

Üniversite, üçüncü taraflar ile yaptığı sözleşmelerde; kişisel verilerin hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi ve verilerin muhafazasını sağlamaya yönelik gerekli yaptırım maddelerini karşılıklı olarak bulundurur. Üçüncü taraflar ile bilgi paylaşımı

yapılmadan önce gizlilik sözleşmeleri imzalanır. Üçüncü taraflara farkındalığın artırılması için gerekli bilgilendirmeler yapılır.

5.1.6. Özel Nitelikli Kişisel Verilerin Koruması İçin Uygulanan Tedbirler

Özel nitelikli kişisel veriler için gerek nitelikleri itibari ile gerekse kişilerin mağduriyetine veya ayrımcılığa yol açabilmesinden dolayı yeterli önlemlerin alınması gerekmektedir. Üniversite, KVK Kanunu ile “özel nitelikli” olarak belirlenen ve hukuka uygun olarak işlenen özel nitelikli kişisel verilerin korunmasında gerekli tedbirleri alır. Kişisel verileri korumak için alınan teknik ve idari tedbirlerde özel nitelikli kişisel veriler için hassasiyet gösterilir. Üniversite işlediği özel nitelikli kişisel verileri KVK Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla işler. Özel nitelikli kişisel veriler işlenmeden önce veri sahibinin açık rızası alınır.

Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde ve Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlara aktarılabilir.

5.1.7. Kişisel Verilerin Korunmasının Sağlanması İçin Farkındalığın Yaratılması

Kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemeye ve muhafazasını sağlamaya yönelik farkındalığın artırılması için birimlere gerekli bilgilendirmeler yapılır, eğitimler düzenlenir ve etkinlikleri ölçülür. “Kişisel Verilerin Korunması ve İşlenmesi Politikası” Üniversitenin web sitesinde yayımlanır. İlgili yasal düzenlemelerde değişiklik olması halinde politikalar revize edilir.

5.2. Kişisel Verilerin İşlenmesi İçin İlkeler

KVK K'nın 4 üncü maddesi 2 inci fıkrasında kişisel verilerin işlenmesi için ilkeler belirlenmiştir. Üniversite belirlenen ilkelere uygun şekilde kişisel verileri işler. Kişisel verilerin işlenmesi aşağıdaki ilkelere uygun yapılır;

- a) Hukuka ve dürüstlük kurallarına uygun olma.
- b) Doğru ve gerektiğinde güncel olma.
- c) Belirli, açık ve meşru amaçlar için işlenme.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

5.3. Kişisel Verinin İşlenmesi Şartları

Üniversite bir kamu kurumu olarak işlediği verilerin önemli bir çoğunluğunu yasal zorunluluklar nedeniyle ve kamu düzeninin korunması için kullanması zorunlu olan yetkileri kullanarak işler. KVKK' nın 5 inci maddesinin 2 inci fıkrası gereği verinin işlenmesinin:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumlarında açık rıza olmaksızın verileri işleyebilir. Bunların dışındaki durumlar için Üniversite ancak veri sahiplerinin açık rızasını temin etmek suretiyle kişisel veri işler.

5.4. Kişisel Verilerin İmhası

Üniversite elde ettiği kişisel verileri kişisel veri sahiplerinin talebi doğrultusunda, yasal zorunluluklar nedeniyle ve kamu düzeninin korunması için kullanması zorunlu değilse imha eder. Veri sahiplerine ait kişisel veriler, hizmetin devam ettirilebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının planlanması gereklilikleri ortadan kalktığında Üniversitenin belirleyeceği imha politikası gereğince imha edilmektedir.

5.5. Kişisel Verilerin Yurtdışındaki Kişilere Aktarılması

Üniversite, kişisel verilerin üçüncü taraflarla paylaşılması hususunda, başka mevzuatta yer alan hükümler saklı kalmak kaydıyla, KVKK'da düzenlenen şartlara uyar. Bu çerçevede, kişisel veriler, veri sahibinin açık rızası olmadan üçüncü kişilere aktarılmaz. Ancak, KVKK'nın 8 inci maddesinin 2 inci fıkrasında düzenlenen şartlardan birinin varlığı halinde kişisel veriler; veri sahibinin açık rızası temin edilmeksizin de aktarılabilir. Özel nitelikli kişisel verilerin aktarılmasında da bu verilerin işleme şartlarında belirtilen koşullara uyulur.

5.6. Kişisel Verilerin Yurtdışındaki Kişilere Aktarılması

Kişisel verilerin yurtdışına aktarılmasına ilişkin olarak, KVKK'nın 9 uncu maddesi doğrultusunda veri sahibinin açık rızası aranır. Ancak, özel nitelikli kişisel veriler dahil, kişisel verilerin veri sahibinin açık rızası olmaksızın işlenmesine izin verilen şartların varlığı halinde, kişisel verinin aktarılacağı yabancı ülkede, yeterli korumanın bulunması kaydıyla veri sahibinin açık rızası aranmaksızın da Üniversite tarafından kişisel veriler yurtdışına aktarılır. Eğer aktarım yapılacak ülke Kurul tarafından yeterli korumanın bulunduğu ülkeler arasında belirlenmemiş ise, Üniversite ve ilgili ülkedeki veri sorumlusu/veri işleyen yeterli korumayı yazılı olarak taahhüt eder. Üniversite yabancı ülkelerdeki sunucularda kişisel veri tutmamaktadır.

5.7. Kişisel Veri Sahibinin Hakları Kişisel Verilerin Korunması Hakkında

Kanun'dan kaynaklanan veri sahibi hakları, KVKK'nın 11 inci maddesinde;

“(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.” şeklinde sıralanmıştır.

Yukardaki maddelerde geçen haklar “Kişisel Veri Sahibi Başvuru Formunu” doldurarak yapılabilir. İlgili Kanun gereği veri sorumlusu ve veri sorumlusu irtibat kişisi bilgileri aşağıdaki şekildedir:

Veri sorumlusu: Niğde Ömer Halisdemir Üniversitesi

Veri sorumlusu irtibat kişisi: Rektör Yardımcısı

5.8. Aydınlatma ve Bilgilendirme Yükümlülüğü

KVKK'nın 10 uncu maddesi kapsamında, veri sahiplerinin, kişisel verilerin elde edilmesinden önce ya da en geç elde edilmesi sırasında aydınlatılması gerekmektedir. Söz konusu aydınlatma yükümlülüğü çerçevesinde veri sahiplerine iletilmesi gereken bilgiler şunlardır:

a) Veri sorumlusunun ve varsa temsilcisinin kimliği.

- b) Kişisel verilerin hangi amaçla işleneceği.
- c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği.
- ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi.
- d) KVKK'nın 11inci maddesinde sayılan diğer haklar.

Öte yandan, KVKK'nın 28 inci maddesinin 1inci fıkrası çerçevesinde, aşağıda sayılan durumlarda aydınlatma yükümlülüğü bulunmamaktadır:

- a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülükler uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.
- b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.
- d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

5.9. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonimleştirilmesi Şartları

Üniversite elde ettiği kişisel verileri kişisel veri sahiplerinin talebi doğrultusunda, yasal zorunluluklar nedeniyle ve kamu düzeninin korunması için kullanması zorunlu değil ise siler, yok eder ya da anonimleştirir.

6. İlgili Dokümanlar

- Kişisel Veri Sahibi Başvuru Formu
- Veri Sorumlusu İrtibat Kişisi Görev Tanımı
- Kişisel Verilerin İşlenmesi Aydınlatma Metni
- Açık Rıza Beyanı