ÇEREZ POLİTİKASI

Ağrı İbrahim Çeçen Üniversitesi olarak, kullanıcılarımızın hizmetlerimizden güvenli ve eksiksiz şekilde faydalanmalarını sağlamak amacıyla sitemizi kullanan kişilerin gizliliğini korumak için çalışıyoruz. Bu kapsamda haklarınızın ve gizliliğinizin teminini sağlamak adına Üniversitemizce işbu Çerez Politikası oluşturulmuştur.

Çerez Politikası, Üniversitemiz tarafından yürütülen internet siteleri ile mobil uygulamalar, üçüncü parti programlar veya internet siteleri üzerinden erişilen, kullanılan platformlar için geçerlidir.

Üniversitemiz internet sitesini kullanarak çerezlerin bu Çerez Politikası ile uyumlu şekilde kullanılmasını kabul etmiş olursunuz. Çerez kullanımını onaylamıyorsanız internet sitesine devam etmemenizi ya da çerez tercihlerinizi bu Politika'da gösterildiği şekilde değiştirmenizi rica ederiz. Çerezlere izin verilmemesi halinde internet sitesinin bazı özelliklerinin işlevselliğini yitirebileceğini hatırlatmak isteriz.

İşbu Çerez Politikası "Kişisel Verilerin Korunması Politikası'nın" ayrılmaz bir parçasıdır. Üniversitemiz tarafından kişisel verilerinizin işlenmesine ilişkin daha detaylı bilgi için "Kişisel Verilerin Korunması Politikamızı" incelemenizi tavsiye ederiz.

Çerez ("Cookie") Nedir?

Çerez (Cookie), internet sitelerinin ziyaretçilerinin bilgisayar veya mobil cihazlarına bıraktıkları küçük boyutlu veri dosyalarına verilen isimdir. Çerezler sanal dünyada geniş çerçevede kullanılan ve web tarayıcılarının otomatik ön kabule tanımlanması sebebiyle ziyaretiniz ile ilgili cihazınızın dil, ayarlar vb. bilgilerinin hatırlanmasına yardımcı olur. İnternet siteleri, kullanıcıların ilk bağlandıklarında oluşturdukları bu veri dosyalarını sonraki bağlanışlarında okuyarak, daha verimli çalışma ve site dili gibi kullanıcı ayarlarını hızlı biçimde yükleme olanaklarına kavuşurlar.

Çerez Türleri Nelerdir?

Çerezler mobil cihazlarda depolanma süreleri ve kimin tarafından yerleştirildikleri gibi kriterlere göre farklı türlere ayrılmaktadır. Bu kriterler kapsamında temel ayrım şu şekildedir:

ÇEREZ TÜRÜ	AÇIKLAMASI
Oturum Çerezleri	Oturum çerezleri, internet sitesini kullanımınız sırasında geçerli olan çerezler olup web tarayıcı kapatılıncaya kadar geçerliliklerini korurlar.
Kalıcı Çerezler	Bu çerezler tarayıcınızda saklanan ve tarafınızdan silininceye dek veya son kullanım tarihine kadar geçerliliğini koruyan çerezlerdir.
Zorunlu Çerezler	İnternet sitesinin düzgün bir şekilde çalışabilmesi, sitenin özelliklerinden ve sunulan hizmetlerden yararlanabilmeniz için kullanımı mecburi olan çerezlerdir.
İşlevsel ve Analitik Çerezler	Tercihlerinizin hatırlanması, internet sitesinin etkin şekilde kullanılması, sitenin isteklerinize cevap verecek şekilde optimize edilmesi gibi amaçlarla kullanılan ve siteyi nasıl kullandığınız hakkında verileri içeren çerezlerdir. Nitelikleri gereği bu türdeki çerezler kişisel verilerinizi içerebilir. Örneğin sitenin görüntülenme dili tercihinizi kaydeden çerezler birer işlevsel çerezdir.

Takip Çerezleri	Takip çerezleri web sitemizi ve üçüncü taraflara ait alan adlarını ziyaretiniz sırasında oluşturulan birincil ve üçüncü taraf çerezlerdir. Bu çerezler oluşturuldukları alan adlarındaki tıklama ve ziyaret geçmişinizin takibini ve farklı alan adları arasında bu kayıtların eşlenmesini mümkün kılmaktadır. Bu tür çerezler kullanıcıların tanınması ve profillenmesi, reklam ve pazarlama faaliyetlerinin hedeflenmesi ve içeriğin özelleştirilmesi amacı ile kullanılmaktadır. Bu çerezler sizin kimliğinizi belirlemek veya şahsınız özelinde karar almak için kullanılmayacaktır.
Birinci Taraf Çerezler	Birinci taraf çerezler ziyaret edilen internet sitesi operatörü tarafından cihaza yerleştirilen çerezlerdir.
Üçüncü Taraf Çerezler	Üçüncü taraf çerezler ziyaret edilen internet sitesi operatörü dışındaki kişiler tarafından cihaza yerleştirilen ve kontrol edilen çerezlerdir.

Çerez Kullanımının Amacı Nedir?

Çerezler birçok farklı hedef için kullanılmaktadır. Bu hedeflerin başlıcaları aşağıda ifade edildiği gibidir:

- İnternet sitesinin işlevselliğini ve performansını arttırmak amacıyla sizlere sunulan hizmetleri geliştirmek,
- İnternet sitesini iyileştirmek ve İnternet sitesi üzerinden yeni özellikler sunmak,
- Ziyaretçiler için daha kişiselleştirilmiş ve daha ilgi çekici bir deneyim sunulabilmek,
- İnternet Sitesinin, kullanıcıların ve Üniversitemizin hukuki ve ticari güvenliğinin teminini sağlamak.
- İlginize yönelik ürün ve hizmet tanıtım çalışması yapabilmek,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve Internet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'ten kaynaklananlar başta olmak üzere, kanuni ve sözleşmesel yükümlülükleri yerine getirilebilmek.

Çerezler Vasıtasıyla Gizli Bilgiler Tutulabilir Mi?

Üniversitemiz, çerezler aracılığıyla kullanıcılarının gizli bilgilerini saklamamaktadır. Çerezler sadece ziyaret geçmişinizle ilgili bilgileri içerir ve bilgisayarınızda veya mobil cihazınızda depolanmış dosyalara erişmez.

Üniversitemiz; işbu Çerez Politikasında kullanıcılarına veya internet sitesi ziyaretçilerine bildirmeksizin değişiklik yapma hakkını haizdir.

Çerezleri Nasıl Kontrol Edebilirsiniz?

Çerezleri dilediğiniz gibi kontrol edebilir veya silebilirsiniz. Cihazınızda hali hazırda mevcut olan çerezleri silebilir ve internet tarayıcınızı çerezleri engelleyebilecek şekilde ayarlayabilirsiniz. Çerezlere ilişkin tercihlerin, ziyaretçinin Platforma erişim sağladığı her bir cihaz özelinde ayrı ayrı yapılması gerekmektedir.

Ancak uyarmak isteriz ki, tarayıcınızı çerezleri engelleyecek şekilde ayarlamanız halinde internet sitemizde yer alan bazı hizmetler gerektiği gibi çalışmayabilir.

Çerezleri kapatmak için;

- Chrome'da tarayıcı ayarlarınızda "Ayarlar/Gizlilik/İçerik Ayarları/Çerez kullanımını kapat" seçeneğini kullanabilirsiniz.

- Internet Explorer kullanıcıları için: “Seçenekler/İnternet Ayarları/Gizlilik/Ayarlar” seçeneklerini kullanabilirsiniz.
- Firefox kullanıcıları için: “Araçlar/ Seçenekler’/Gizlilik/ Çerez kabul yöntemi/Firefox kapatılana kadar” seçeneklerini kullanabilirsiniz.
- Safari kullanıcıları için: “Tercihler/Gizlilik/ Web Sitesi Verileri/Bir veya daha fazla web sitesini seçin/Tümünü sil” seçeneğini kullanabilirsiniz.
- Opera kullanıcıları için: “Tercihler/Gelişmiş/Çerezler” seçeneğini kullanabilirsiniz.

AĞRI
İBRAHİM ÇEÇEN
ÜNİVERSİTESİ
2007

KİŞİSEL VERİ İHLALİ DİSİPLİN POLİTİKASI

1.GİRİŞ

İşbu politika, Üniversitemizce Kişisel Verileri Koruma Kurumu (KVKK) Kişisel Veri Güvenliği Rehberi'nde yayımlanan ve veri sorumluları tarafından alınması gereken idari ve teknik tedbirler ışığında veri sorumlusunun alması gereken idari tedbirlerden biri olan kurum içi disiplin yönetmeliğinin hazırlanması ve uygulamaya konulması amacıyla hazırlanmıştır.

Ağrı İbrahim Çeçen Üniversitesi Disiplin Politikası çerçevesinde;

Üniversite çalışanlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatta yer alan düzenlemeler ve Ağrı İbrahim Çeçen Üniversitesi Kişisel Verilerin Korunması Politika ve Prosedürlerine ilişkin uymaları gereken kurallar ve yükümlülükler ile bu kuralların ihlali halinde uygulanacak prosedürler düzenlenmektedir.

Bilindiği üzere ;

KVKK 17. Maddesi: "(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır." hükmünü havidir.
5237 sayılı Türk Ceza Kanunu'nun 135. maddesinde, kişisel verilerin kaydedilmesi suçu, 136. maddesinde, verileri hukuka aykırı olarak verme veya ele geçirme suçu, 138. maddesinde, verileri yok etmeme suçları düzenlenmiştir. Ayrıca Kanunun 140. maddesinde bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik tedbirlerinin uygulanacağı hükme bağlanmıştır. İlgili madde düzenlemelerine göre:

TCK m. 135 – ***Hukuka aykırı olarak kişisel verileri kaydeden kimseye 6 aydan 3 yıla kadar hapis cezası verilir.***

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olan kişisel verilerinin hukuka aykırı şekilde kayda alınması suçun oluşması için yeterlidir. **Kişisel verilerin kişilerin siyasi, felsefi, dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantıları ile ilgili olması durumunda cezanın yarı oranında arttırılacağı öngörülmüştür.**

TCK m. 136 – ***Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, 2 yıldan 4 yıla kadar hapis cezası ile cezalandırılır.***

Bu madde ile birlikte hukuka aykırı olarak kişisel verileri bir başkasına vermek, yaymak ve ele geçirmek fiilleri suç olarak nitelendirilmiştir. Yukarıdaki maddelerde tanımlanan suçlara ilişkin olarak aşağıdaki maddede bu suçların nitelikli halleri düzenlenmiştir.

TCK m. 137 –Nitelikli haller

Kamu görevlisi tarafından ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle,

Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle

İşlenmesi halinde, verilecek ceza yarı oranında artırılır.

TCK m. 138 –

Kanunların belirlediği sürelerin geçmiş olmasına karşın ***verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde 1 yıldan 2 yıla kadar hapis cezası verilir.***

Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek ceza bir kat artırılır.

İşbu sebeple kişisel veri ihlalinin gerçekleştirildiği, kanun kapsamına giren fillerde Türk Ceza Kanunu kapsamında hapis cezası yaptırımı gündeme gelebilecektir. İhlale ilişkin olarak Üniversitemizce öngörülen diğer yaptırımlar bu politikada düzenlenmektedir.

2. TANIMLAR VE KISALTMALAR

ÜNİVERSİTE:	**Ağrı İbrahim Çeçen Üniversitesi**
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.

ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Kişisel Veri İhlali Disiplin Politikası
KVK KOMİTESİ:	Kişisel Verilerin Korunması Komitesi. Üniversitemiz tarafından atanmış Kişisel Verilerin Korunması Kanunu ve alt düzenlemeleri kapsamında oluşturulmuş süreçlerin idari takibini yapmak üzere oluşturulan komite.
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

3.AMAÇ

Kişisel Veri İhlali Disiplin Politikası ("Politika") , Üniversitemizce işlenen kişisel verilerin ihlali halinde Üniversitemiz tarafından benimsenecek ve uygulamada dikkate alınacak disiplin prosedürlerini belirlemek amacıyla hazırlanmıştır.

4. KAPSAM

İşbu politika, Üniversitemizin tam zamanlı, yarı zamanlı, kısa süreli ve diğer tüm çalışanları için deneme süresi dâhil tüm çalışma süresince bağlayıcıdır.

5.GÖREV VE SORUMLULUKLAR

- Tüm Üniversite çalışanları işbu Disiplin Politikası ve Kişisel Verilerin Korunmasına ilişkin Kişisel Verilerin Korunması Politikası, Özel Nitelikli Kişisel Verilerin Korunması Politikası, Kişisel Veri Saklama ve İmha Politikası ve Bilgi Güvenliği Politikası başta olmak üzere, mevcut politika,

prosedür ve talimatlar kapsamında düzenlenen kuralların uygulanmasından ve bunlara uyulmasından sorumludur.

- Her birim yöneticisi kendisine bağlı çalışanlara işbu Disiplin Politikası kapsamında kuralların aktarılmasından, bu kurallara uyulmasının takibinden ve gerekli hallerde uyarılarda bulunulmasından, bu kuralların güncellenmesi ihtiyacını fark etmeleri durumunda insan kaynakları bölümünü ve Kişisel Verilerin Korunması Komitesi'ni bilgilendirmekten sorumludur.
- Disiplin Kurulu, Disiplin Politikasına ilişkin kararlarının alınması aşamasında Kişisel Verilerin korunması Politikası ve prosedürlerine uygun hareket edilmesinden ve kendilerine gelen dosyaların gizliliğinden sorumludur.

6.UYGULAMA

- Çalışan, iş görme borcunu 6698 Sayılı Kişisel Verilerin Korunması Kanunu uyarınca ve 4857 sayılı İş Kanunu'nda hüküm altına alınan işçinin işi kendisinin yapması, işin özenle yapılması, itaat borcu, sadakat borcu, rekabet etmeme borcuna ve işveren tarafından yürürlüğe konulacak işyeri politika ve prosedür hükümleri gereğince yerine getirmekle yükümlüdür.
- Çalışanının bu yükümlülüğünü ihlal ettiği durumlarda disiplin süreci başlatılacaktır.
- Disiplin prosedürü başlatma kararı alınmadan önce, Üniversite yetkilileri durumu iyice araştıracaktır. Bu kapsamda çalışanın yazılı e-postaları ve telefonu incelenebilir.
- Soruşturma başladıktan/tamamlandıktan sonra yetkili kişi, çalışana hakkında aleyhinde başlatılan soruşturma hakkında bilgi verecektir.
- Gerekli görülen durumlarda çalışanın bilgisayarı, e-postaları ve telefonu incelenebilir. Soruşturma başladıktan/tamamlandıktan sonra yetkili kişi, çalışana hakkında aleyhinde başlatılan soruşturma hakkında bilgi verilir.

7.ŞARTLAR

- Üniversite'nin tüm çalışanları, başta İş Kanunu ve Kişisel Verilerin Korunması Kanunu hükümlerine ve yaşanan olayın niteliğine göre ilgili kanun ve yönetmeliklere göre hareket edecektir.
- Kişisel Verilerin Korunmasına ilişkin; Kişisel Verilerin Korunması Politikası, Özel Nitelikli Kişisel Verilerin Korunması Politikası, Kişisel Veri Saklama ve İmha Politikası ve Bilgi Güvenliği Politikası başta olmak üzere, mevcut politika, prosedür ve talimatlarına uyulmaması halinde, İş Kanunu ve Kişisel Verilerin Korunması Kanunu'nda yer alan hükümler ile ihtiyaç duyulması halinde 5237 sayılı Türk Ceza Kanunu hükümleri uygulanacaktır.
- İş Kanunu hükümlerine tabi olmayan personelin kurumla aralarındaki sözleşmelerde yer alan hükümler uygulanacaktır. Aksi durumda genel hukuk kurallarına tabi olacaktır. Kurum hizmet aldığı yükleniciler ile de kurumsal gizlilik sözleşmesi imzalanacaktır.
- Üniversite politikasına uyma yükümlülüğü bulunan taraflar, Üniversite içinde denetim ile görevli personel veya Üniversite dışından alınan denetim hizmetleri kapsamında, yukarıdaki maddelerde belirlenen kurallara uygun kullanımının, kullanıcının kişilik hakları saklı kalmak üzere, kontrol edebileceğinden haberdardır ve bunu açıkça kabul eder.
- Kullanıcılar, kurum bünyesinde çalışmaya başladığı zaman Üniversite ile İş Sözleşmesi imzalarlar ve sözleşmede yazan tüm hususlara uymayı kabul ve taahhüt ederler.

- Üniversite'nin vermiş olduğu her türlü hat, telefon, tablet, e-posta, bilgisayar Üniversite'nin malıdır ve gerekli görülen her durumda önceden bildirim yapılmaksızın çalışandan alınıp içerisinde bulunan her bir veri incelenebilir.
- Çalışanlar, Üniversite amaçları dışında gerekli olmayan materyalleri indiremez ve kullanamaz.
- E-postalar özel amaçlarla kullanılamaz ve Üniversite işi dışındaki herhangi bir amaçla kullanılamaz.
- Tüm yazılımlar Üniversite'ye aittir, çalışanlar tarafından kopyalanamaz.
- Çalışan herkes internet güvenliği, verilerin gizliliği ve kişisel verilerin korunması ile ilgili protokol ve yönergelere uymak zorundadır.
- Çalışanlar, Üniversite hakkındaki herhangi bir uygunsuz bilgiyi internete yüklemeyecek, e-posta veya diğer iletişim araçları ile paylaşmayacaktır.
- E-postalar, internet ve diğer elektronik iletişim yöntemleri tamamen güvenli değildir, n belirlemiş olduğu şifreleme yöntemi ile güvenlik sağlanacaktır.
- Üniversite'de bulunan donanımlar Üniversite'nin malı olup bunlara verilecek zararlar kanun nezdinde suç teşkil eder.
- Donanımın dış görünüşünü değiştirmek, bağlı parçaların bağlantı şeklini değiştirmek, parçaları çalmak veya çalmaya teşebbüs etmek gibi eylemler gerçekleştiğinde yetkili birim ve kişiler tarafından tutanak tutulur, disiplin soruşturması açılır. Ek olarak kullanıcı hesabı süresiz kapatılır. Üniversitemiz avukatı aracılığı ile söz konusu davranışlarda bulunan kişiler hakkında yetkili makamlara şikâyette bulunur.
- Üniversite tarafından herhangi bir etkinliğin tehlikeli olduğu kanaatine varılması halinde bu etkinlik engellenebilir, okunabilir, takip edilebilir ve analiz edilebilir.
- Çalışanlar, Üniversite bünyesinde yer alan bilgileri, sırları ve kişisel verileri ifşa etmemekle yükümlüdürler.
- Üniversite, herhangi bir çalışana kullanımı amacıyla temin etmiş olduğu dolabı ve/veya aracı istediği zaman arama hakkını saklı tutar. Çalışanın aramaya karşı gelmesi Üniversite politikasını ciddi suiistimal sayılır.
- Ağ ihlalleri gizlilik ihlali kabul edilecektir.
- Disk alanında zararlı dosyalar bulundurulması durumunda kullanıcı hesabı süresiz kapatılır ve dosyalar silinir.
- Başkalarının alanlarına erişilmesi durumunda kullanıcı hesabı süresiz kapatılır, kanuni süreç başlatılır, disiplin soruşturması açılır.
- Her türlü kişisel şifreyi paylaşmak disiplin soruşturması gerektirir. Şifresini paylaşan her türlü sorumluluğu kabul etmiş sayılır.
- Başkasının e-posta hesabını kullanılması durumunda kullanıcı hesabı süresiz kapatılır.
- Hakaret içerikli e-posta gönderilmesi durumunda kullanıcı hesabı süresiz kapatılır, kanuni süreç başlatılır, disiplin soruşturması açılır.
- Kurum tarafından sağlanan e-posta hizmeti kullanılarak devlet sırrı niteliğindeki her türlü bilgi ve evrak, Know-how üçüncü şahıslarla paylaşılması durumunda kanuni girişimlerde bulunulur ve disiplin süreci başlatılır.
- Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir.
- KVK komitesi bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile işbirliği yapar. Bunun dışındaki kural ihlallerinde disiplin soruşturması açılır. Gerekli görülmesi halinde İş Kanunu hükümleri uyarınca iş akdi feshedilebilir ve kural ihlallerinin suç unsuru oluşturması halinde kişi, meydana getirmiş olduğu eylemin cezai sorumluluğundan mesul olur.

- İhlalin tespit edildiği durumlarda tutanak tutularak Kişisel Verilerin Korunması Komitesi'nin konu hakkında görüşü alınır. Disiplin cezaları, karar tarihinden itibaren hüküm ifade eder ve uygulanır.

8.DİSİPLİN CEZALARI

8.1. Yazılı İhtar

Çalışanın, 4857 sayılı İş Kanunu'nun 25. maddesi uyarınca haklı nedenle derhal feshe neden olacak ağırlıkta bulunmamakla birlikte, iş sözleşmesine ve kanunlara aykırı davranışları, fiziki ve mesleki yetersizliği, işyerinin normal işleyişini ve yürüyüşünü bozan, iş görme borcunun gerektiği şekilde yerine getirilmesini engelleyen, iş yerindeki uyumu olumsuz yönde etkileyen, Üniversite gizli bilgilerinin ve müşterilerin kişisel verilerinin korunması yükümlülüğüne yönelik prosedürlere aykırı hareket etmesi hallerinde yazılı olarak uyarılması ve savunmasının alınmasıdır.

Çalışan, dikkat çekme ve uyarı niteliğindeki yazılı ihtar sonrasında tanıklar huzurunda yazılı olarak savunma vermediği ve/veya imtina ettiği takdirde uyarı sebebinin haklılığını kabul ve ikrar etmiş sayılır.

Bu cezanın verilmesinde komitenin kararına gerek olmaksızın, çalışanın bağlı olduğu birim yöneticisi tek başına yetkilidir. Çalışana tebliğ edilen yazının bir örneği sicil dosyasına konulmak üzere İnsan Kaynaklarına gönderilir. Yazılı ihtar, bir sonraki aşamada davranış ve/veya yükümlülüğün yerine getirilmemesi durumunda iş akdinin feshedilebileceğini açıkça ifade edecektir.

Yazılı İhtar Gerektiren Durumlar:

- Görev ve sorumluluklarını yerine getirmemek, ilgisizlik ve düzensizlik göstermek,
- Üniversite varlık ve teçhizatının izinsiz kullanımı,
- Kişisel verilerin korunması ile ilgili prosedürlere aykırı davranışlar sergileyerek, ceza alınması veya tazminat ödenmesini gerektirmeyen küçük ihlallerde bulunmak,
- E-posta hesabını iş dışındaki mailler için kullanmak,
- Üniversite politikalarını veya prosedürlerini uygulamada kasıt bulunmayan zarara sebep olmayan hata yapmak,
- İşyerinde açıkça duyurulmuş ve uygulanmakta olan prosedür ve yönetmeliklere uymamak,
- Üniversite'nin uygulanmasını kabul ettiği loglama yöntemini kasıt bulunmaksızın uygulamamak,
- Kişisel veri içeren e-maili kasıt bulunmaksızın yanlış birime göndermek,
- Kişisel veri içeren belgeyi kasıt bulunmaksızın imha etmemek,
- 6698 sayılı kanun çerçevesinde Kişisel Verilerin Korunması Komitesi/Yetkilisi tarafından Üniversite genelinden yayınlanan makul talimatlara uymayı reddetmek,
- Gerektiğinde yöneticileri tarafından kendisinden istenen rapor, bilgi, belge vb. zamanında vermemek veya yanlış bilgi vermek,
- Kendi sorumluluğunda olan donanım, yazılım, makine, malzeme ve tesisata gerekli özeni göstermemek,
- Yukarıda anılmayan ve İş Kanunu'na göre derhal feshe neden olacak ağırlıkta bulunmayan her türlü hallerde yazılı ihtar verilebilir.

Bu liste sınırlı sayıda olmayıp, her olay kendi içerisinde buradaki örneklemelerden faydalanılarak ayrıca ele alınacaktır. Yazılı ihtar cezası kişinin performans değerlendirmesinde, terfi veya görev değişikliklerinde ve iş sözleşmesinin feshi hallerinde dikkate alınır.

8.2. Kınama

Çalışanın, iş görme borcunu 4857 sayılı İş Kanunu'nda hüküm altına alınan çalışanın işi kendisinin

yapması, işin özenle yapılması, itaat borcu, sadakat borcu, rekabet etmeme borcuna riayet ederek, çalışmalarındaki tavır ve davranışlarında geliştirmesi gereken yanlarıyla ilgili yazılı olarak kınanmasıdır.

Çalışanın işi özenle yapması, itaat borcu, özel haller, kuruma sadakat borcu, rekabet etmeme borcu kapsamına 6698 sayılı Kişisel Verilerin Korunması Kanunu ile getirilen hükümler de dahildir. Kınama, kınama ve ağır kınama olmak üzere iki biçimde uygulanır.

Kınama Cezasını Gerektiren Durumlar:

- En az 2 defa Kişisel Verilerin Korunması Kanunu'na kasıt bulunmaksızın aykırı davranışlarda bulunmak suretiyle yazılı ihtar almak,
- Üniversite politikası ve prosedürlerinde düzenlenen hassas nitelikte bulunan kişisel verilerin korunması, aktarılması ve imha edilmesine yönelik yöntemlere aykırı davranmak,
- Üniversite'ye ait verileri ve bilgileri ortaya çıkarıp, dışarı aktarmak, yetkisiz kişi veya birimlere aktarmak, kötüye kullanmak,
- Çalışanın Üniversite'nin herhangi bir mülkünü, tesisini veya kullanım yetki alanında bulunan yerlerin dışındaki yerlere yetkisiz olarak erişmesi,
- Özellikle güvenliği sağlamak için tasarlanmış kurallar, politikalar veya prosedürlerin ciddi şekilde ihlali,
- E-posta, telefon, sesli mesaj ve bilgisayar sistemlerinin yetkisiz kullanımı,
- Yönetimi altındaki çalışanın yönetim ve denetimine gereken dikkati göstermeyerek Üniversite politika ve prosedürlerine aykırı davranışlar yapılmasına elverişli bir ortamın doğmasına yol açmak,
- Birlikte çalıştığı çalışanın suç sayılabilecek hal ve hareketlerini zamanında yöneticilerine bildirmekten kaçınmak,
- Kullanılması veya muhafazası kendisine bırakılmış olan makine ve tesisata gerekli özeni göstermeyerek hasara uğratmak ve/veya kaybetmek,
- İşyeri tarafından kullanımına verilmiş her türlü şifreyi başkasına açıklamak, kullanımına izin vermek veya başkasına ait şifreyi kullanmak.

Bu liste sınırlı sayıda olmayıp, her olay kendi içerisinde buradaki örneklemelerden faydalanılarak ayrıca ele alınacaktır. Kınama cezası bir yıl süre ile terfi etmeyi engeller. Çalışan yıl içinde ödenen her türlü primden ve/veya ödenekten yoksun kalır ve kınama cezası, kişinin performans değerlendirmesinde dikkate alınır.

Ağır Kınama Cezasını Gerektiren Durumlar:

- Çalışanları etkileyebilecek herhangi bir suç işlenmesi veya Üniversite için mahkûmiyet ya da para cezasına neden olacak davranışlarda bulunulması,
- İlgisizlik ve dikkatsizlik nedeniyle yanlış ve/veya eksik işlem yaparak veya görevin gerektirdiği işlemleri geciktirerek işyerini zarara sokmak ve/veya güç duruma düşürmek,
- Görevli olmadığı halde makine, donanım, fiziksel veya bilgisayar ortamındaki bilgileri karıştırmak ve bu durumun gizliliğini ihlal etmek suretiyle bu bilgileri başkalarıyla paylaşmak,
- Prosedüre uygun olarak verilen talimatları yerine getirmemek veya eksik yapmak suretiyle işyerini zarara sokmak,
- Kasıtlı olarak üstlerine yanlış bilgi vermek, bildirilmesi gereken hususları saklamak veya disiplin kurulu ya da soruşturmalarda gerçeğe aykırı bildirimde bulunmak, haklı bir neden bulunmaksızın ifade vermekten kaçınmak veya soruşturmayı güçleştirmek,

- İşyeri dahilinde yapılan bir Üniversite'yi zarara sokan eylemi, suç oluşturan eylemi veya Üniversite politika ve prosedürlerine ağır aykırılık içeren kasıtlı bir eylemi bilerek haber vermemek,
- Müşterilere, çalışanlara ve tedarikçilere ait bilgilerin gizliliği ilkesine uymamak,
- Görevli olmadığı halde basın ve/veya medyaya kurumla ilgili açıklamalarda bulunmak,
- İşyerine ilişkin her türlü kişisel veri barındıran bilgi ve belgeleri 3. şahıs ve/veya kurumlarla paylaşmak.

Ağır kınama cezası 2 yıl süre ile terfi etmeyi engeller, çalışan yıl içinde ödenen her türlü primden yoksun kalır ve kişinin performans değerlendirmesinde dikkate alınır

8.3. Görevden Çıkarma

4857 sayılı İş Kanunundan doğan fesih hakkı saklı kalmak üzere çalışanın, bir daha işyerinde çalıştırılmamak üzere iş akdinin fesih edilmesidir.

Görevden Çıkartma Cezasını Gerektiren Haller:

- Kasıtlı olarak her türlü kişisel veriyi dışarı aktarmak, düzenlemelere aykırı olarak imha etmek, imha edilmesi gereken veriyi imha etmemek,
- İş akdi yapıldığı sırada gerçeğe aykırı bilgi ve belgelerle işyerini yanıltmak ve verilerini gerçeğe uygun güncellememek,
- İş sözleşmesinde yer alan uyulması zorunlu ve çalışan tarafından da kabul edilmiş yükümlülükleri yerine getirmemek,
- Kişisel veri sahiplerine ait bilgileri resmi mercilerin yasal taleplerine verilecek cevap dışında, veri sahibinin rızası dışında üçüncü kişilere açıklamak yoluyla gizlilik ilkesini ihlal etmek,
- İşyeri tarafından kendisine verilmiş her türlü şifreyi başkasına açıklamak, kullanımına izin vermek veya başkasına ait şifreyi izinli veya izinsiz kullanmak suretiyle işyerinin zararına neden olmak,
- Kişisel veri barındıran her türlü belge, bilgi ve dokümanı tahrip etmek, ettirmek veya kötü niyetle yok etmek veya ettirmek, sahte belge düzenlemek, yetkisiz kişiye veya yetkisiz birime aktarmak,
- Görev yetkisi dışında bulunan birimin kişisel verilerine kasıtlı olarak erişmek,
- Görevli olmadığı halde makine, donanım, fiziksel veya bilgisayar ortamındaki bilgileri karıştırmak ve bunları başkalarıyla paylaşmak suretiyle kuruma zarar vermek, Bu liste sınırlı sayıda olmayıp, her olay kendi içerisinde buradaki örneklemelerden faydalanılarak ayrıca ele alınacaktır.

9.DİSİPLİN CEZALARINA İLİŞKİN GENEL HÜKÜMLER

Çalışan tarafından, işbu Disiplin Politikasında yer alan kurallarda tanımlı olmayan, ancak Üniversite bünyesindeki uyumlu ve verimli çalışma ortamını zedeleyecek, bozacak tavır ve/veya davranışın sergilenmesi durumunda, disiplin yönetmeliğinde yer alan ve ona en yakın ve/veya benzer madde üzerinden işlem yapılır.

9.1. Benzer Hal ve Eylemler

Çalışan tarafından, Disiplin Politikasında yer alan kurallarda tanımlı olmayan, ancak Üniversite bünyesindeki uyumlu ve verimli çalışma ortamını zedeleyecek, Üniversite'nin itibarını bozacak tavır ve/veya davranışın sergilenmesi durumunda, Disiplin Politikasında yer alan ve ona en yakın ve/veya benzer madde üzerinden işlem yapılır.

9.2. Tekrar

Kişilerin, prosedür kapsamındaki kurallara aykırı düşen tavır, davranış ve olayları tekrarlaması durumunda bir üst ceza uygulanır.

Zarar karşılığı kesinti kuruma verilen maddi zarar, kişinin bir aylık ücretinin (bu ücrete primler ve hakedişler ile ek kazançlar da dahildir) ¼ ünden fazla olmamak koşuluyla eşit taksitlendirilerek ücretinden ve/veya hak edişlerinden kesilir.

Bu prosedürün uygulanmasında 4857 Sayılı İş Kanunu'nun, 6698 sayılı Kişisel verilerin Korunması Kanunu'nun ve 5237 sayılı Türk Ceza Kanunu'nun ve 6098 Sayılı Türk Borçlar Kanunu'nun ilgili madde hükümlerinin uygulanma hakkı saklı tutulur.

9.3.Öngörülmemiş Disiplin Suçları

Yukarıda sayılan ve disiplin cezası verilmesini gerektiren fiil ve hallere, nitelik ve ağırlıkları itibariyle benzer eylemlerde bulunanlara da aynı türden disiplin cezaları verilir.

9.4. Toplu Olarak İşlenen Disiplin Suçları

Toplu olarak işlenen disiplin suçlarında, suçluların münferiden tespit edilemediği durumlarda, topluluğu oluşturan üyelerin her birine ceza verilir.

9.5. Cezalarda Ağırlaştırıcı ve Hafifleştirici Sebepler

Disiplin cezası verilmesine neden olmuş bir fiil veya halin tekrarında bir derece ağır ceza uygulanır.

Aynı derecede cezayı gerektiren, fakat ayrı fiil ve haller nedeniyle verilen disiplin cezalarının üçüncü uygulamasında da bir derece ağır ceza verilir. Toplu suç işleme ağırlaştırıcı sebep sayılır ve bu durumda bir derece ağır ceza verilir.

Disiplin cezalarının verilmesinde tahrik ve suç işleme kastının bulunmaması gibi durumlar hafifletici neden sayılabilir ve bir derece hafif ceza verilebilir.

10.SORUMLULAR

Üniversite bünyesinde faaliyet gösteren tüm personel bu sürecin işletilmesinden sorumludur.

11.İLGİLİ DÖKÜMANLAR

Veri İhlali Müdahale Politikası

12. REVİZYON TABLOSU

Revizyon No	Revizyon Tarihi	Değişen Sayfa	Açıklama

AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ 2007

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI POLİTİKASI

1.BÖLÜM

1.1 GİRİŞ

Ağrı İbrahim Çeçen Üniversitesi tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") uyarınca kişisel verilerin hukuka uygun olarak korunması ve işlenmesine azami önem verilmekte vetüm planlama ve faaliyetlerde bu özenle hareket edilmektedir. Üniversite, kişisel verilerin korunmasına ilişkin gerekli olan tüm idari ve teknik tedbirleri dikkatle almaktadır. Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki veriler olduğundan, özel nitelikli kişisel verilerin niteliği ve hassasiyeti uyarınca bu verilerin işlenmesi, korunması ve güvenliğine ilişkin olarak genel nitelikteki kişisel veriler için alınan idari ve teknik tedbirlere ek olarak özel nitelikli teknik ve idari tedbirler alınmaktadır.

1.2.AMAÇ

İşbu Özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası **("Politika")**, özel nitelikli kişisel verilerin işlenmesine, korunmasına ve güvenliğine ilişkin olarak Anayasa, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, ilgili mevzuat, Kişisel Verileri Koruma Kurulu'nun 31.01.2018 Karar Tarihli ve 2018/10 Karar No'lu kararı ve diğer ilgili kararları çerçevesinde gerekli teknik ve idari tedbirleri almak ve Üniversite'nin veri sorumlusu sıfatıyla elinde bulundurduğu özel nitelikli kişisel verilere ilişkin olarak yükümlülüklerini yerine getirmesini sağlayarak İlgili Kişileri bilgilendirmektir.

1.3. KAPSAM

İşbu Politika, Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve üçüncü kişiler ile herhangi bir nedenle Üniversitemiz nezdinde özel nitelikli kişisel verisi bulunan tüm gerçek kişileri ve bunların özel nitelikli kişisel verilerinin işlenmesine, korunmasına ve güvenliğine yönelik yürütülen faaliyetleri kapsamaktadır.

Üniversite bünyesinde, özel nitelikli kişisel verilerin işlendiği tüm kayıt ortamları ve özel nitelikli kişisel verilerin tamamen veya kısmen otomatik olan yollarla veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesine yönelik faaliyetlerde işbu Politika uygulanmaktadır.

1.4. TANIMLAR VE KISALTMALAR

ÜNİVERSTİTE:	**Ağrı İbrahim Çeçen Üniversitesi**
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.

İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.
ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle

	değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

2.BÖLÜM

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI, İŞLENMESİ, İŞLENME AMAÇLARI VE İŞLENMESİNE İLİŞKİN TEMEL İLKELER

2.1. 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 özel nitelikli kişisel verilerdir.

2.2. Özel Nitelikli Kişisel Verilerin Korunması

Özel nitelikli kişisel veriler, öğrenilmesi halinde İlgili Kişi hakkında ayrımcılık yapılmasına veya mağduriyetine neden olabilecek nitelikte veriler olduğundan, hukuka uygun şekilde işlenen bu kişisel verilerin korunması hususunda Üniversite tarafından alınan idari ve teknik tedbirler özel nitelikli kişisel veriler bakımından özenle uygulanmakta ve Üniversite bünyesinde gerekli denetimler yapılmaktadır. Bunun yanında özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemler alınarak, gerekli işlemler yürütülmektedir.

2.3 Özel Nitelikli Kişisel Verilerin İşlenmesi

İlgili Kişi açısından korunmasının çeşitli açılardan daha kritik önem teşkil ettiğine inanılan özel nitelikli kişisel verilerin işlenmesinde ise Üniversite tarafından özel hassasiyet gösterilmektedir. Özel nitelikli kişisel veriler Üniversitemiz tarafından, işbu Politika'da belirtilen ilkelere uygun olarak ve Kurul'un belirleyeceği yöntemler de dahil olmak üzere gerekli her türlü idari ve teknik tedbirler alınarak ve aşağıdaki şartların varlığı halinde işlenmektedir:

(i) Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmesi diğer bir ifade ile ilgili faaliyetin tabi olduğu kanunda kişisel verilerin işlenmesine ilişkin açıkça bir hüküm olması halinde veri sahibinin açık rızası aranmaksızın işlenebilecektir. Aksi durumda söz konusu özel nitelikli kişisel verilerin işlenebilmesi için veri sahibinin açık rızası alınacaktır.

(ii) Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, 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 kuruluşlar tarafından açık rıza aranmaksızın işlenebilecektir. Aksi durumda söz konusu özel nitelikli kişisel verilerin işlenebilmesi için veri sahibinin açık rızası alınacaktır.

2.4. Özel Nitelikli Kişisel Verilerin İşlenme Amaçları

Özel nitelikli kişisel veriler, Kanun'un 4. maddesinde belirtilen ilkelere ve ilgili mevzuatta yer alan usul ve esaslara uygun olarak, Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları doğrultusunda işlenebilmektedir. Üniversitemiz tarafından usulüne uygun yöntemlerle toplanan özel

nitelikli kişisel veriler iş ilişkisi, ürün, hizmet veya ticari faaliyetler kapsamında veya İlgili Kişiler ile olan diğer ilişkiler dâhilinde, işlenmelerini gerektiren aşağıdaki amaçlar çerçevesinde, bu amaçlarla bağlantılı, sınırlı ve ölçülü olarak işlenmekte ve saklanabilmektedir.

Özel nitelikli kişisel verilerin işlenme amaçları;

- Üniversitemizin ortaya koymuş olduğu her türlü faaliyetten faydalananlar için gerekli çalışmaların, ilgili iş birimleri tarafından yapılması,
- Yükseköğretim Kanunu, ilgili ikincil düzenlemeler ve Yükseköğretim Kurumu (YÖK) tarafından getirilen eğitim faaliyetlerine ve denetime ilişkin ve sair yükümlülüklerin karşılanması,
- Eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık faaliyetlerinin sürdürülmesi, yükseköğretim mevzuatı ve Üniversitemiz iç düzenlemeleri kapsamında eğitim faaliyetinden kaynaklı hakların tesis edilmesi, kimlik kartı üretimi, basımı ile çeşitli akademik ve idari işlemlerin yapılması,
- Üniversitemizin stratejilerinin belirlenmesi ve uygulanması, Üniversitemizin ve faaliyetlerinin tanıtılması, Üniversitemizin insan kaynakları politikalarının yürütülmesi,
- İlgili bölümlerde eğitim gören ve Üniversite bünyesindeki birimlerde veya üniversite dışındaki kuruluşlarda staj yapan öğrencilerin hak ve yükümlülüklerinin korunması ve yerine getirilmesinin sağlanması,
- Üniversite öğrenci topluluklarından birisine üye olunması halinde, toplulukların bağlantıda olduğu dernek, vakıf, sivil toplum kuruluşları ile Üniversite tarafından Kanunlarda ön görülen kayıtların tutulması amacıyla işlenmesi, gerekli olması halinde kanunen yetkili kamu kurum, kuruluş ve özel kişilerle paylaşılması,
- Üniversite öğrencilerinin, çalışanlarının, ziyaretçilerinin can ve mal güvenliğinin korunması veya bu maddede belirtilenlere ilişkin kurallara uyum sağlanması da dâhil olmak üzere, yasal yükümlülüklerin, yargı organlarının veya yetkili idari kuruluşların talep veya gerekliliklerin yerine getirilmesi,
- Verilerin, gerekli güvenlik ve hukuki önlemler alınarak burada bahsedilen amaçların gerçekleştirilmesi için bilgi işlem altyapılarına, elektronik veya fiziki ortamlarda yasal yükümlülüklerin yerine getirilmesi amacıyla arşivlenmesi,
- Listeleme, raporlama, doğrulama, analiz ve değerlendirmeler yapmak, İstatistikî ve bilimsel bilgilerin üretilmesi,
- İlişkide bulunulan kişilerin internet sitesi, web uygulamaları, mobil uygulamalar ve diğer iletişim kanallarını, kullanım şekillerine ilişkin analiz yapması ve özelleştirmelerde bulunulması,
- Üniversite'nin ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Üniversite tarafından yürütülen finans operasyonları, iletişim, pazar araştırmaları ve sosyal sorumluluk aktiviteleri ile talep, teklif, değerlendirme, sipariş, bütçe, sözleşme gibi satın alma operasyonlarının yürütülmesi,
- Üniversite içi sistem ve uygulama yönetimi operasyonları ile hukuki operasyonların yönetilmesi,

- Üniversite ile ilişkisi bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) Üniversitemiz ve/veya Üniversitemize bağlı merkez ve birimlerinin ürün ve hizmetlerinden yararlanabilmeleri için gerekli çalışmaların ilgili birimleri tarafından yapılabilmesi,
- Üniversite ana kampüsü ve/veya bağlı merkez ve birimlerinde bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) can ve mal güvenlikleri ile hukuki, ticari ve iş sağlığı güvenliklerinin temini,
- 2547 sayılı Yükseköğretim Kanunu, 4857 sayılı İş Kanunu, 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu, 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 3308 sayılı Mesleki Eğitim Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 213 sayılı Vergi Usul Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 3359 sayılı Sağlık Hizmetleri Temel Kanunu, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, Özel Hastaneler Yönetmeliği, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Korunması Yönetmeliği vb. ilgili tüm kanunlardan ve ikincil düzenlemelerden doğan/doğabilecek yasal ve düzenleyici gereksinimlerin yerine getirilmesi ve bu kapsamda gerekli tedbirlerin alınabilmesi,
- Üniversitemizin ve Üniversitemizle ilişki içerisinde olan üçüncü, gerçek veya tüzel kişilerin hukuki ve ticari güvenliğinin temini ve bunlarla yapılan sözleşmeler veya yürütülen faaliyetler çerçevesinde, hukuki ve ticari yükümlülüklerin gerçekleştirilmesi,
- Üniversite tarafından iş ortağı, müşteri, tedarikçiler ve çalışanlarla yapılan sözleşmelerden kaynaklanan yükümlülüklerin ifası, hak tesisi, hakların korunması, ticari ve hukuki değerlendirme süreçleri, hukuki ve ticari risk analizleri, hukuki uyum süreci, mali işlerin yürütülmesi,
- Görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca yapılacak denetleme ve/veya düzenleme görevlerinin yürütülmesi,
- Öğrenciler ile akademik ve idari personel hakkında açılan/açılabilecek disiplin soruşturması süreçlerinin yönetilebilmesi,
- Üniversite bünyesinde bulunan öğrenci kulüplerine üye olunabilmesi, kulüp çatısı altında yapılan çalışmalardan, etkinliklerden ve organizasyonlardan yararlanılabilmesi; ayrıca dernek, vakıf, sivil toplum kuruluşu ve/veya sendikalarla herhangi bir işbirliği ve/veya bağlantısı bulunan bir kulübe üye olunması halinde, bu üyelik ile ilgili kanunlarda öngörülen kayıtların tutulabilmesi,
- Yargı organlarının ve/veya idari makamların istediği bilgi ve belge taleplerinin yerine getirilmesi,
- Üniversite ve Üniversiteye bağlı tüm merkez ve birimlerde sunulan ürün ve hizmetlerin kullanım şekline ilişkin listeleme, raporlama, doğrulama analiz çalışması yapmak, bu hususta istatistiki ve bilimsel bilgiler üretmek, buna bağlı olarak ürün ve hizmetlerimizi geliştirmek, ürün ve hizmetlerimize ilişkin memnuniyeti arttırmak ve bu kapsamda kullanıcıya ilişkin özelleştirmelerde bulunmak,

- Akademik eğitimler, bilimsel araştırmalar, proje başvuruları, Fikri ve Sınai Mülkiyet Kanunu kapsamındaki haklara ilişkin başvuru, devir vb. her türlü işlemler ile yayın, danışmanlık vb. her türlü faaliyetin sürdürülebilmesi,
- Üniversite ile Üniversiteye bağlı merkez ve birimlerin akreditasyon ve değerlendirme çalışmalarının yapılabilmesi,
- Kamu düzeninin ve sağlığının korunması,
- Koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım, medikal malzemelerinin temini gibi sağlık hizmetlerinin yürütülmesi ve yönetilmesi,
- Sunulan tüm hizmetlerin finansmanının planlanması ve yönetimi, faturalandırılmasının yapılması,
- Tüm çalışanların eğitilmesi ve geliştirilmesi,
- Eğitim, seminer vb. organizasyonlara katılım taleplerinin yerine getirilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Anlaşmalı olunan özel sigorta şirketleri ve/veya diğer kurumlar tarafından, anlaşmalar çerçevesinde sunulan teklif, promosyon, muafiyet vb. hak ve yükümlülüklerin yerine getirilmesi,
- Hukuki uyum süreçlerinin yürütülmesi,
- Operasyonların yönetimi,
- Mali ve finansal işlerin yerine getirilmesi,
- Ticari ve iş stratejilerinin belirlenmesi ve yerine getirilmesi,
- Hizmet sözleşmesine bağlı olarak; hizmet yükümlülüklerinin yerine getirilmesi,
- Acil durum yönetimi süreçlerinin yürütülmesi,
- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,
- Çalışanlar için yan haklar ve menfaatleri süreçlerinin yürütülmesi,,
- Çalışanlar için iş faaliyetlerinin yürütülmesi,
- Çalışanların başvuru süreçlerinin değerlendirilmesi,
- Faaliyetlerin mevzuata uygun yürütülmesi,
- İnsan kaynakları faaliyetinin planlanması,
- İş sağlığı / güvenliği faaliyetlerinin yürütülmesi,
- Yetkili kişi, kurum ve kuruluşlara haber verilmesi.

2.5. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Üniversite bakımından öncelikle önem arz eden hususlardan biri, özel nitelikli kişisel verilerin işlenmesinde mevzuatta öngörülen genel ilkelere uygun davranılmasıdır. Bu kapsamda, Üniversite, Anayasa ve KVK Kanunu'na uygun olarak özel nitelikli kişisel verilerin işlenmesinde aşağıda sıralanan ilkelere uygun hareket etmelidir.

a. Hukuka ve Dürüstlük Kuralına Uygun Kişisel Veri İşleme Faaliyetlerinde Bulunma

Üniversite, KVK Kanunu'nun 4. maddesine uygun olarak, özel nitelikli kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde özel nitelikli kişisel veri işleme faaliyetinde bulunmaktadır. Bu kapsamda Üniversite, özel nitelikli kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta ve özel nitelikli kişisel verileri amacın gerektirdiği durumlar dışında kullanmamaktadır.

b. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama

Üniversitemiz, İlgili Kişinin temel haklarını ve kendi meşru menfaatlerini dikkate alarak işlediği özel nitelikli kişisel verilerin doğru ve güncel olmasını sağlamakta; bu doğrultuda gerekli tedbirleri alarak bunları sağlamaya yönelik sistemleri kurmaktadır.

c. Belirli, Açık ve Meşru Amaçlarla İşleme

Üniversite, özel nitelikli kişisel verileri meşru ve hukuka uygun sebeplerle ve yürütmekte olduğu faaliyetlerle bağlantılı olarak ve gerekli olduğu ölçüde işlemektedir. Üniversite tarafından özel nitelikli kişisel verilerin hangi amaçla işleneceği henüz kişisel veri işleme faaliyeti başlamadan belirlenmektedir.

d. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Üniversite, özel nitelikli kişisel verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işlemekte ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınmaktadır. Üniversitemizce sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik özel nitelikli kişisel veri işleme faaliyeti yürütülmemektedir.

e. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Etme

Üniversite, Türk Ceza Kanunu'nun 138.maddesine ve KVK Kanunu'nun 4. ve 7. maddelerine uygun olarak; işlediği özel nitelikli kişisel verileri, yalnızca ilgili mevzuat ve kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar muhafaza etmektedir.

Bu kapsamda, Üniversitemiz öncelikle ilgili mevzuatta özel nitelikli kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmaktadır. Yasal bir süre mevcut değil ise özel nitelikli kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Özel nitelikli Kişisel veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya İlgili Kişi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir. Detaylar, Kişisel Verileri Saklama ve İmha Politikası'nda belirtilmiştir.

3. BÖLÜM

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI VE ŞARTLARI:

3.1. Özel Nitelikli Kişisel Verilerin Aktarılması

Üniversitemiz, özel nitelikli kişisel verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte olmaları sebebiyle,

hukuka uygun olarak işlediği bu tür kişisel verilerin aktarılması süreçlerinde de gerekli önlemleri hassasiyetle almaktadır. Bu kapsamda Üniversitemiz, özel nitelikli kişisel verileri işleme amaçları doğrultusunda, mevzuata uygun olarak gerekli idari ve teknik tedbirleri alarak üçüncü kişilere aktarabilmektedir.

3.2. Özel Nitelikli Kişisel Verilerin Aktarım Şartları

a. Özel Nitelikli Kişisel Verilerin Yurt İçine Aktarım Şartları:

Üniversitemiz, özel nitelikli kişisel verileri ilgili kişinin açık rızası olması koşuluyla, veri işleme amaçları doğrultusunda ve mevzuat uyarınca gerekli teknik ve idari tedbirleri alarak yurt içindeki üçüncü kişilere aktarabilmektedir. Özel nitelikli kişisel veriler kural olarak İlgili Kişinin açık rızası olmaksızın yurt içindeki üçüncü kişilere aktarılamaz.

Ancak sağlık ve cinsel hayat dışındaki kişisel veriler kanunlarda açıkça öngörülmesi halinde, diğer bir ifade ile ilgili faaliyetin tabi olduğu kanunda özel nitelikli kişisel verilerin işlenmesine/aktarılmasına ilişkin açık bir hüküm olması halinde İlgili Kişinin açık rızası aranmaksızın aktarılabilir. Bu doğrultuda sağlık ve cinsel hayata ilişkin kişisel veriler dışındaki özel nitelikli kişisel veriler:

- Veri Sahibi'nin açık rızası var ise,
- Kanunlarda Özel Nitelikli Kişisel Veri'nin aktarılacağına ilişkin açık bir düzenleme var ise,
- Veri Sahibi'nin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve Veri Sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Üniversite'nin hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Özel Nitelikli Kişisel Veriler, Veri Sahibi tarafından alenileştirilmiş ise,
- Özel Nitelikli Kişisel Veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Veri Sahibi'nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Üniversite'nin meşru menfaatleri için kişisel veri aktarımı zorunlu ise aktarılabilmektedir.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise yeterli ve gerekli önlemler alınarak ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amaçlarından herhangi birinin bulunması halinde İlgili Kişinin açık rızası aranmaksızın aktarılabilir.

b. Özel Nitelikli Kişisel Verilerin Yurt Dışına Aktarım Şartları:

Üniversite, gerekli özeni göstererek, mevzuatın öngördüğü idari ve teknik tedbirler ile Kurul tarafından gerekli görülen önlemleri alarak, meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda özel nitelikli kişisel verileri yurt dışına aktarabilmektedir. Özel nitelikli kişisel veriler kural olarak İlgili Kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

Ancak sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmesi halinde, diğer bir ifade ile ilgili faaliyetin tabi olduğu kanunda kişisel verilerin işlenmesine/aktarılmasına ilişkin açık bir hüküm olması halinde İlgili Kişinin açık rızası aranmaksızın, Kurul tarafından belirlenerek

ilan edilen yeterli korumaya sahip ülkelere aktarılabilmektedir. Yeterli korumanın bulunmaması halinde ise ancak veri sorumlularının yeterli korumayı taahhüt etmeleri ve Kurul'un izninin bulunması halinde yurt dışına veri aktarımı yapılabilmektedir.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amaçlarından herhangi birinin bulunması halinde İlgili Kişinin açık rızası aranmaksızın, Kurul tarafından belirlenerek ilan edilen yeterli korumaya sahip ülkelere aktarılabilmektedir. Yeterli korumanın bulunmaması halinde ise ancak veri sorumlularının yeterli korumayı taahhüt etmeleri ve Kurul'un izninin bulunması halinde yurt dışına veri aktarımı yapılabilmektedir.

4.BÖLÜM

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ

Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine Üniversitemiz tarafından silinir, yok edilir veya anonim hale getirilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanun'un 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve Kişisel Veri Saklama ve İmha Politikası' na uygun hareket edilmektedir.

5.BÖLÜM

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN GÜVENLİĞİ

Özel nitelikli kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12. maddesinde belirtilen yükümlülüklere uygun olarak ve 6. maddesinin dördüncü fıkrası uyarınca özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Üniversite tarafından gerekli teknik ve idari tedbirler alınmaktadır.

Bu kapsamda Kişisel Verilerin İşlenmesi ve Korunması Politikası ile Kişisel Verileri Saklama ve İmha Politikası'nda Üniversite tarafından alınan teknik ve idari tedbirler belirlenmiştir. Üniversite özel nitelikli kişisel verilerin işlenmesi, güvenliği ve korunması faaliyetlerinde bu politikalarda belirtilen teknik ve idari tedbirlere ek olarak ayrıca aşağıdaki tedbirleri almaktadır.

5.1. Özel Nitelikli Kişisel Verilerin İşlenme Süreçlerinde Yer Alan Çalışanlara Yönelik Tedbirler:

- İlgili mevzuat ile özel nitelikli kişisel verilerin işlenmesi, güvenliği, korunması, saklanması vb. veri güvenliği konularında çalışanlara eğitimler verilmektedir.
- Çalışanlarla gizlilik sözleşmeleri yapılmakta ve disiplin prosedürleri uygulanmaktadır.
- Özel nitelikli kişisel verilere erişim yetkisine sahip çalışanların, yetki kapsamları ve süreleri tanımlanmaktadır.
- Periyodik olarak yetki kontrolleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılmaktadır. Bu kapsamda, varsa kendisine tahsis edilen envanter geri alınmaktadır.

5.2. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği ve/veya Erişildiği Elektronik Ortamlara İlişkin Tedbirler:

- Veriler kriptografik yöntemler kullanılarak muhafaza edilmektedir.
- Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulmaktadır.
- Veriler üzerinde gerçekleştirilen hareketlerin işlem kayıtları güvenli olarak loglanmaktadır.
- Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilmekte, güvenlik testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır.
- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanmaktadır.
- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi uygulanmaktadır.

5.3. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği ve/veya Erişildiği Fiziksel Ortamlara İlişkin Tedbirler:

- Özel nitelikli kişisel verilerin bulunduğu fiziksel ortamlar (dolap, arşiv vs.) kilitlenmektedir.
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmaktadır.
- Bu ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

5.4. Özel Nitelikli Kişisel Verilerin Aktarılmasına İlişkin Tedbirler:

- Özel nitelikli kişisel verilerin e-posta yoluyla aktarılması gerekiyorsa, bu veriler şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmaktadır. Söz konusu dosyanın şifre bilgisine posta içeriğinde yer verilmemektedir.
- Özel nitelikli kişisel verilerin taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa, bu veriler kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır.
- Özel nitelikli kişisel verilerin aktarımı farklı fiziksel ortamlardaki sunucular arasında gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.
- Özel nitelikli kişisel verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa, bu verilerin aktarıldığı evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizlilik dereceli belgeler" formatında gönderilmektedir.

6.BÖLÜM

6.1 POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

Özel nitelikli kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında

uyumsuzluk bulunması durumunda, Üniversite yürürlükteki mevzuatın uygulama bulacağını kabul etmektedir.

Politika, ilgili mevzuat tarafından ortaya konulan kuralları Üniversite uygulamaları kapsamında somutlaştırarak düzenlemektedir. Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

6.2. POLİTİKA'NIN YÜRÜRLÜĞÜ

İşbu Politika'nın yürürlük tarihi 31.12.2021'dir. İşbu Politika, Üniversite'nin www.agri.edu.tr internet sitesinde yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

6.3.DAĞITIM

Politika, Üniversite internet sitesinde yayınlanarak, Üniversite'nin idari yetkililerine, akademik ve idari personeline, öğrencilerine, mezunlarına, personel adaylarına, öğrenci adaylarına, ziyaretçilerine, iş birliği içinde olduğu kurumların çalışanlarına ve diğer üçüncü kişilere duyurulur.

AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ 2007

TEMİZ EKRAN TEMİZ MASA POLİTİKASI

TEMİZ EKRAN TEMİZ MASA POLİTİKASI

1.AMAÇ

Kişisel verilerin korunması, Ağrı İbrahim Çeçen Üniversitesi'nin ("Üniversite ") en önemli öncelikleri arasında olup, bu hususta yürürlükte bulunan tüm mevzuata uygun davranmak için azami gayret gösterilmektedir. İşbu Temiz Ekran Temiz Masa Politikası ("Politika") ile Üniversitemizce işlenen kişisel verilerin teknik ve idari açıdan korunması sağlanmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verinin korunması konusunda bağlayıcı yükümlülükler ve neticesinde yaptırımlar öngörmektedir. Bu kapsamda kişisel verinin korunması ciddi önem arz etmektedir.

Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Çalışanların mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri ortadan kaldırmaktır.

Bu politika Üniversite personeli için yazılmış olup, güvenlik sorumlulukları olan tüm departman ve çalışanlar için geçerlidir.

2.UYGULAMA

- Hassas bilgiler içeren evraklar, bilgi ve belgeler masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulundurulmamalıdır.
- Çalışma saatleri sonunda ise masaüstünde herhangi bir doküman bulundurulmamalıdır.
- Bu bilgi ve belgeler kilitli yerlerde muhafaza edilmelidir.
- Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.
- Ofisten uzun süreli ayrılmalar öncesinde, çalışma masası ve çevre ünitelerinde evrak temizliği yapılmalıdır.
- Çalışma ortamlarındaki yazı tahtaları kullanıldıktan sonra temizlenerek bırakılmalıdır.
- Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmamalıdır.
- Önemli dokümanlar dolaplara ve kilitli çekmecelere kaldırılmalıdır.

- Kullanım ömrü sona eren ve artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yalana vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.
- Personel, bilgisayara ve/veya işletim sistemine şifre tanımlamalı, bilgisayar başından kalkarken mutlaka oturumu kilitlemeli, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlamalıdır.
- Tüm bilgisayar oturumları parola korumalı olup, bilgisayar boş kaldığında 5 (Beş) dakika içerisinde otomatik olarak kilitlenecek konuma getirilmelidir.
- Sistemlerde kullanılan şifre, telefon numarası ve T.C Kimlik numarası gibi bilgiler ekran üstlerinde veya masaüstünde bulundurulmamalıdır.
- Çalışma saatleri dışında bilgisayar kapalı ve uyku durumunda bırakılmalıdır.
- Çalışma saatleri içerisinde bilgisayar başından ayrılırken bilgisayar mutlaka kilitli bırakılmalıdır.
- Bilgisayar ekranları ve klavyeler kullanıcısı haricindeki kişilerin göremeyeceği şekilde konumlandırılmalıdır.
- Taşınabilir medya ve mobil cihazlar daima kullanıcısının yanında bulundurulmalıdır. Kullanılmadığı durumlarda mutlaka kilitli dolaplarda muhafaza edilmelidir.
- Masaüstlerinde Üniversite'ye ait bilgi içeren dokümanlar kilitli ortamda tutulmalıdır.
- Gelen ve giden mesaj noktaları, faks veya teleks makinalarındaki mesajlar başıboş olarak bırakılmamalıdır.
- Üniversite'ye ait antetli kağıtlar kilitli ortamlarda tutulmalıdır.
- Yazdırma işlemi yapan kişi yazıcıdaki çıktıyı kendi kontrolüne almalıdır. Hassas ve sınıflandırılmış bilgi uzak ağ yazıcılarından yazdırılmamalıdır.
- Uzak yazıcılardan yazdırma yapılacak ise parola korumalı yazdırma özelliği kullanılmalıdır. Şifreler kağıt, yapışkan kağıt ve ajanda gibi matbu ortamlarda yazılı olarak bulundurulamamalıdır.
- Her türlü bilgiler şifreler anahtarlar ve bilginin sunulduğu sistemler (sunucu, dizüstü ve masaüstü bilgisayarlar vb. cihazlar) yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ 2007

KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

1.BÖLÜM

1.1 GİRİŞ

Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin birinci fıkrasına göre ;

"Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmü yer almaktadır.

Bu kapsamda, kişisel verilerin işlenmesi sürecinde alınması gereken teknik ve idari tedbirler konusunda alınması gereken önlemleri tanımlamak amacıyla bu politika hazırlanmıştır.

1.2.KAPSAM

Üniversite'nin 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 kişilere ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Üniversite'nin sahip olduğu ya da Üniversitemizce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. HEDEF

Üniversite Kişisel Veri Güvenliği Politikası ile Üniversite bünyesinde kişisel verilerin hukuka uygun olarak işlenmesi ve korunması konusunda farkındalığın oluşması hedefi doğrultusunda gerekli sistemleri oluşturmak ve mevzuata uyumu temin etmek için gereken düzenin kurulması amaçlanmaktadır.

2. BÖLÜM

2.1. TANIMLAR VE KISALTMALAR

ÜNİVERSİTE	**Ağrı İbrahim Çeçen Üniversitesi**
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.
ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Üniversite Kişisel Veri Güvenliği Politikası
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

3.BÖLÜM

KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN İDARİ TEDBİRLER

3.1. Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Bu riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.

3.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.

Kişisel veri güvenliğini ihlal etmeye yönelik saldırıların yanısıra, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu ihlaller, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinin kullanılması suretiyle kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde de ortaya çıkabilmektedir.

Bu nedenle çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.

Tüm çalışanların hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.

Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesine dikkat edilmelidir.

Öte yandan, çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşmalarını imzalamaları istenebilir. Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci de mutlaka olmalıdır.

Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; yapılacak yeni eğitimlerle bu değişikliklerin, çalışanların bilgisine sunulması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulması sağlanmalıdır.

Her bir kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.

3.3. Kişisel Verilerin Mümkün Olduğunca Azaltılması

Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Ancak, çok fazla miktarda kişisel veri toplamakta olduğundan söz konusu kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir. Bunun önüne geçebilmek için, işleme amaçları bakımından anılan kişisel verilere hala ihtiyaç olup olmadığının değerlendirilmesi ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olunması gerekmektedir.

Bunun yanında, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

3.4. Veri İşleyenler ile İlişkilerin Yönetimi

Hizmet alınan veri işleyenlerin kişisel veriler konusunda sağladığı güvenlik seviyesinin yeterli olduğundan emin olunmalıdır. Zira Kanunun 12 nci maddesinin ikinci fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur. Veri işleyen ile imzalanan sözleşmenin yazılı olması, veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin

korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hüküm içermesi ve Kişisel Veri Saklama ve İmha Politikasına uygun olması gereklidir.

Veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağının da bu sözleşmede yer alması önem taşımaktadır.

Ayrıca; taraflar arasındaki sözleşmenin niteliği buna elverdiği ölçüde, veri işleyene aktarılan kişisel veri kategori ve türlerinin de ayrı bir maddede belirtilmiş olması, veri işleyenin veri güvenliğini sağlama yükümlüğünü yerine getirmesi açısından faydalı olacaktır. Bununla birlikte kişisel veri içeren sistem üzerinde gerekli denetimler düzenli olarak yapılmalı veya yaptırılmalıdır, denetim sonucunda ortaya çıkan raporlar ve hizmet sağlayıcı yerinde incelenebilir.

4.BÖLÜM

KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER

4.1. Siber Güvenliğin Sağlanması

Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında öncelikli olarak güvenlik duvarı ve ağ geçidi tedbiri alınmalıdır. Güvenlik duvarının iyi yapılandırılması, kullanılmakta olan ağa derinlemesine nüfuz etmeden önce, gerçekleşen ihlalleri durdurması açısından çok önemlidir.

Çalışanların kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önleyebilmek için İnternet ağ geçidi kullanılmalıdır. Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikli olarak tercih edilmelidir.

Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleridir. Yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir. Ayrıca, kişisel veri içeren sistemlere erişim sınırlı olmalıdır.

Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmalıdır. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmalıdır.

Buna bağlı olarak veri sorumlularının, erişim yetki ve kontrol matrisi oluşturmaları ve ayrı bir erişim politika ve prosedürleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınması önerilmektedir.

Güçlü şifre ve parola kullanımının yanısıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişikleri kesilen çalışanlar için zaman

kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılması gerekmektedir.

Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır. Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanması için önemlidir.

4.2. Kişisel Veri Güvenliğinin Takibi

Sistemlere içeriden veya dışarıdan gelen saldırılar ve siber suçlar veya kötü amaçlı yazılımlara maruz kalma durumunda, müdahale için geç kalmadan;

- Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
- Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
- Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
- Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
- Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir.

Söz konusu raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir. Ayrıca güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir.

Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

4.3. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Üniversite yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanan kişisel verilerin, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunması gerekmektedir.

Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınması önemlidir. Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılmalı veya bileşenlerin ayrılması sağlanmalıdır. Kullanılmakta olan ağın sadece belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.

Aynı seviyedeki önlemlerin Üniversite yerleşkesi dışında yer alan kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir. Kişisel veri güvenliği ihlalleri sıklıkla kişisel

veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi gerekmektedir.

Ayrıca çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için de mutlaka yeterli güvenlik tedbirleri alınmalıdır. Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulmalı, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler de alınmalıdır.

Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır.

Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmalı, söz konusu evraklara yetkisiz erişim önlenmelidir. Bunlarla birlikte şifreleme farklı farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracıdır. Bu kapsamda, tam disk şifrelemesiyle cihazın tümü şifrelenebilir ya da cihazda bulunan bir dosya şifrelenebilir.

Bazı yazılımlar ise verilerde değişiklik yapılmasına izin vermemek için şifre koruması sunmakla birlikte bu yazılımlar kişisel verinin yetkisiz kişiler tarafından okunmasını durdurmaz. Bu nedenle hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir. Tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem gösterilmelidir.

4.4.Kişisel Verilerin Bulutta Depolanması

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü kapsamında Üniversite'ye ait bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu durum birtakım riskleri beraberinde getirmektedir. Bu nedenle, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının değerlendirilmesi gerekmektedir. Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması gerekmektedir.

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir.

Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekir.

4.5.Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

Yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir.

Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır. Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılması gerekir. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

4.6.Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir. Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir.

Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi gerekir. Yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmalıdır.

5.BÖLÜM

ÖZET TABLOLAR

5.1.Teknik Tedbirler Özet Tablosu

Teknik Tedbirler
Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

5.2.İdari tedbirler Özet Tablosu

İdari Tedbirler
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ 2007

KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI POLİTİKASI

1.BÖLÜM

1.1 GİRİŞ

Kişisel verilerin korunması, Ağrı İbrahim Çeçen Üniversitesi'nin ("Üniversite ") en önemli öncelikleri arasında olup, bu hususta yürürlükte bulunan tüm mevzuata uygun davranmak için azami gayret gösterilmektedir. İşbu Kişisel Verilerin Korunması ve İşlenmesi Politikası ("Politika") çerçevesinde Üniversitemiz tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin yürütülmesinde benimsenen ilkeler ve Üniversitemizin veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("Kanun") yer alan düzenlemelere uyumu bakımından benimsenen temel prensipler açıklanmakta ve böylelikle Üniversitemiz, kişisel veri sahiplerini bilgilendirerek gerekli şeffaflığı sağlamaktadır. Bu kapsamdaki sorumluluğumuzun tam bilinci ile kişisel verileriniz işbu Politika kapsamında işle nmektedir.

1.2.AMAÇ

Üniversitemiz, Kişisel Verilerin Korunması ve İşlenmesi Politikası doğrultusunda, kişisel verilerin korunmasına ilişkin Türkiye Cumhuriyeti Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), sair mevzuat tarafından getirilmiş ilke, kurallara uymayı ve ilgili kişilerin haklarını korumayı taahhüt etmektedir. Bu amaçla, uygulanmak ve geliştirilmek üzere yazılı bir kişisel veri koruma politikası ve sistemi benimsemiştir.

Kişisel Verilerin İşlenmesi ve Korunması Politikası ile kişisel verilerin korunması ve işlenmesi konusunda Üniversite tarafından benimsenecek ve uygulamada dikkate alınacak ilkeler ortaya konulmaktadır.

Politika, Üniversite olarak kişisel verilerin korunması ve işlenmesi konusunda 6698 Sayılı Kişisel Verilerin Korunması("KVK") Kanunu'na uyum sağlamak amacıyla yürütülecek uyum faaliyetlerinin çerçevesini belirlemeyi ve koordinasyonu sağlamayı hedeflemektedir.

Bu kapsamda amaç; Üniversite'nin kişisel verilerin yönetiminde kendi standartlarını oluşturması ve gerçekleştirmesinin sağlanması; organizasyonel hedef ve yükümlülüklerin belirlenmesi ve desteklenmesi, Üniversite'nin kabul edilebilir risk seviyesiyle uyumlu olarak kontrol mekanizmalarının tesis edilmesi; faaliyetlerin hukuka uygunluk, dürüstlük ve şeffaflık ilkelerine uygun olarak yürütülmesinin sürdürülmesi ile Üniversite'nin kişisel verilerin yönetiminde kendi standartlarını oluşturması ve gerçekleştirmesinin sağlanması ve Üniversite'nin kişisel verilerin korunması alanındaki uluslararası sözleşmeler, Anayasa, kanunlar, sözleşmeler ve meslek kuralları uyarınca tabi olduğu yükümlülüklerin yerine getirilmesi ve bireylerin menfaatlerinin en iyi şekilde korunmasıdır.

İşbu politika, başta Üniversite'nin 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 kişileri kapsar.

Politika ile, Üniversite'nin kişisel verilerin korunmasına yönelik benimsemiş olduğu ilkeler ve kurmuş olduğu sistemler konusunda bilgilendirerek şeffaflığı sağlamak amaçlanır.

1.3. KAPSAM

İşbu politika, KVKK ve sair mevzuata teknik ve idari konularda uyum sağlamak için gerçekleştireceği düzenlemelere esas teşkil etmek üzere hazırlanmıştır. Üniversite'nin tüm akademik ve idari çalışanları görevlerini yerine getirirken işbu politika ile getirilen düzenlemeler ile KVKK ve sair mevzuat hükümlerine uygun hareket etmekle yükümlüdür.

Bu politika, başta Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler ve Üniversite tarafından işlenen tüm kişisel veriler ve özel nitelikli kişisel verileri kapsamaktadır.

2. BÖLÜM

2.1. TANIMLAR VE KISALTMALAR

ÜNİVERSİTE:	Ağrı İbrahim Çeçen Üniversitesi
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.

VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.
ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası
ÖĞRENCİ ADAYI	Üniversitemize herhangi bir yolla ulaşmış, bilgilerini Üniversitemizin incelemesine açmış olan gerçek kişiler
ÖĞRENCİ	Kişisel verilerini eğitim maksadıyla Üniversitemizin incelemesine açmış olan gerçek kişiler
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Üniversite Kişisel Verilerin Korunması Ve İşlenmesi Politikası.
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

2.2.İLGİLİ KİŞİ KAVRAMI- İŞLENEN KİŞİSEL VERİLERİN SINIFLANDIRILMASI

İLGİLİ KİŞİLER:

Kanun kapsamında "İlgili Kişi" kişisel verisi işlenen gerçek kişiyi ifade etmekte olup, işbu politika kapsamında ilgili kişiler – sayılanlarla sınırlı kalmamakla birlikte – aşağıdakileri kapsamaktadır;

- Öğrenci, Personel ve diğer otomasyonlarımız veri tabanında kayıtlı tüm katılımcılar,
- Üniversitemiz çalışanları,
- Ağrı İbrahim Çeçen Üniversitesi öğrencileri,
- Daha önce Üniversitemiz bünyesinde çalışmış fakat herhangi bir sebeple iş sözleşmesi sona ermiş olan eski çalışanlar,
- Üniversitemize iş başvurusunda bulunmak amacıyla kariyer portallarından İŞKUR, e-posta veya referans aracılığı ile fiziki olarak başvuru formu dolduran veya Ağrı İbrahim Çeçen Üniversitesi web sitesi aracılığı ile özgeçmiş gönderen çalışan adayları,
- Üniversitemiz iletişim seçeneklerinden herhangi birini kullananlar,
- Üniversitemiz web sitesini kullanan tüm kullanıcılar,
- Üniversitemizin ihtiyaç analizleri ve hizmet memnuniyetleri kapsamında düzenlemiş olduğu anketlere katılanlar,
- Ağrı İbrahim Çeçen Üniversitesi mobil uygulamalarını kullanan tüm kullanıcılar,
- Ağrı İbrahim Çeçen Üniversitesi sosyal medya hesaplarından Üniversitemiz ile iletişime geçen (yorum paylaşan, talepte bulunan dâhil ve bunlarla sınırlı olmamak kaydıyla) tüm kişiler, kurum ve kuruluşlar,
- Üniversitemizin misafir ağına (wi-fi) bağlanan tüm kullanıcılar,
- Üniversitemiz faaliyetleri kapsamında çalışılan tüm yükleniciler ve çalışanları,
- Üniversitemiz iştirakleri/paydaşları ve çalışanları,
- Üniversitemiz ile iş yapan tüm tedarikçi firmalar,
- Herhangi bir sebeple Üniversitemizi ziyaret eden tüm ziyaretçiler,
- Stajyerler ve kursiyerler,

Yukarıda belirtilenlerle sınırlı olmaksızın yüz yüze, mesafeli, sözlü, yazılı ya da elektronik yolla kişisel verilerini Üniversitemiz ile paylaşmış/paylaşacak; doğrudan vermiş/verecek veya Ağrı İbrahim Çeçen Üniversitesi tarafından elde edilmesine olanak sağlamış/sağlayacak olan tüm gerçek kişiler.

KİŞİSEL VERİLER:

Kişisel veriler; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgilerdir.

Kişisel verilerin korunması sadece gerçek kişiler ile ilgili olup tüzel kişilere ait, içerisinde gerçek kişiye ilişkin bilgi içermeyen bilgiler kişisel veri korunması dışında bırakılmıştır. Bu nedenle işbu Politika tüzel kişilere ait verilere uygulanmaz.

Kurumumuzun meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda, Kanun'da düzenlenen bütün yükümlülüklere uyularak aşağıda belirtilen kategorilerdeki kişisel veriler, Kanun uyarınca ilgili kişiler bilgilendirilmek suretiyle işlenmektedir.

2.2.1. Veri Tipi Kategorileri;

Kişisel Veri Kategorileri	Alt Başlıklar ve Açıklamalar
Kimlik	Ad soyad, T.C. kimlik numarası, uyruk bilgisi, anne adı-baba adı, anne kızlık soyadı, doğum yeri, doğum tarihi, cinsiyet gibi bilgileri içeren ehliyet, nüfus cüzdanı ve pasaport gibi belgeler ile vergi numarası, SGK numarası, imza bilgisi, taşıt plakası v.b. bilgiler.
İletişim	İletişim bilgileri; telefon numarası, adres, e-mail adresi, faks numarası vb. kişisel verilerdir.
Aile Bireyleri ve Akraba/Yakın Bilgisi	Üniversite tarafından yürütülen faaliyetler çerçevesinde, sunulan hizmetlerle ilgili veya Üniversite'nin ve kişisel veri sahibinin hukuki ve diğer menfaatlerini korumak amacıyla işlenen kişisel veri sahibinin aile bireyleri (örn. eş, anne, baba, çocuk), yakınları ve acil durumlarda ulaşılabilecek diğer kişiler hakkındaki bilgiler.
Özlük	Kurum çalışanlarına ait bordro bilgileri, disiplin soruşturması, işe giriş-çıkış belgesi kayıtları, özgeçmiş bilgileri, performans değerlendirme raporları vb.
Hukuki İşlem	Adli Makamlarla yazışma bilgileri, dava dosyalarındaki bilgiler.
İşlem Güvenliği Bilgisi	Sorumluluklarımız kapsamında faaliyetlerimizi yürütürken teknik, idari, hukuki güvenliğimizi sağlamamız için işlenen kişisel veriler vb.
Fiziksel Mekan Güvenliği	Çalışanların ve ziyaretçilerin, öğrencilerin giriş çıkış kayıtları, kamera kayıtları.
İşlem Güvenliği	İnternet sitesi giriş çıkış bilgileri, Ip adresi bilgileri, şifre ve parola bilgileri.
Hizmet Bilgisi	Hizmetlerimizin kişisel veri sahibinin hizmet alma alışkanlıkları, beğenisi ve ihtiyaçlarına yönelik işlenen kişisel veriler ve bu işleme sonuçlarına göre yaratılan rapor ve değerlendirmeler vb
Mesleki Deneyim	Diploma bilgileri, gidilen kurslar, Meslek içi eğitim bilgileri, transkript bilgileri, sertifikalar.
Dernek, Vakıf, Sendika Üyeliği	Dernek, vakıf, sendika üyeliği bilgileri
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	Ceza mahkûmiyetine ilişkin bilgiler, güvenlik tedbirlerine ilişkin bilgiler
Görsel ve İşitsel Kayıtlar	Görsel ve işitsel kayıtlar
Özel Nitelikli Kişisel Veriler	KVKK'nın 6. maddesinde belirtilen veriler (örneğin; kan grubu da dahil sağlık verileri, biyometrik veriler, din ve üye olunan dernek bilgisi gibi).
Talep/Şikayet Yönetimi Bilgisi	Kuruma yöneltilmiş olan her türlü talep veya şikayetin alınması ve değerlendirilmesine ilişkin kişisel veriler ve bu işleme sonuçlarına göre yaratılan rapor ve değerlendirmeler vb.

Özel Nitelikli Kişisel Veriler:

Kişilerin, ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları ile kılık ve kıyafeti, dernek, vakıf ya da sendika üyelikleri, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir.

2.3.KİŞİSEL VERİLERİN BULUNDUĞU ORTAMALAR

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

2.4.KİŞİSEL VERİLERİN İŞLENME AMAÇLARI:

Kişisel Verilerin Elde Edilme, İşlenme ve Kullanılma Amaçları

Üniversitemizce işlenen kişisel veriler, KVKK' nın 4. 5. ve 6. maddeleri uyarınca; aşağıda belirtilen amaçlarla işlenmektedir:

- Üniversitemizin ortaya koymuş olduğu her türlü faaliyetten faydalananlar için gerekli çalışmaların, ilgili iş birimleri tarafından yapılması,
- Yükseköğretim Kanunu, ilgili ikincil düzenlemeler ve Yükseköğretim Kurumu (YÖK) tarafından getirilen eğitim faaliyetlerine ve denetime ilişkin ve sair yükümlülüklerin karşılanması,
- Eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık faaliyetlerinin sürdürülmesi,
- Yükseköğretim mevzuatı ve Üniversitemiz iç düzenlemeleri kapsamında eğitim faaliyetinden kaynaklı hakların tesis edilmesi, kimlik kartı üretimi, basımı ile çeşitli akademik ve idari işlemlerin yapılması,
- Üniversitemizin stratejilerinin belirlenmesi ve uygulanması,
- Üniversitemizin ve faaliyetlerinin tanıtılması,
- Üniversitemizin insan kaynakları politikalarının yürütülmesi,

- İlgili bölümlerde eğitim gören ve Üniversite bünyesindeki birimlerde ve ya Üniversite dışındaki kuruluşlarda staj yapan öğrencilerin hak ve yükümlülüklerinin korunması ve yerine getirilmesinin sağlanması,
- Üniversite öğrenci topluluklarından birisine üye olunması halinde, toplulukların bağlantıda olduğu dernek, vakıf, sivil toplum kuruluşları ile Üniversite tarafından kanunlarda ön görülen kayıtların tutulması amacıyla işlenmesi, gerekli olması halinde kanunen yetkili kamu kurum, kuruluş ve özel kişilerle paylaşılması,
- Üniversite öğrencilerinin, çalışanlarının, ziyaretçilerinin can ve mal güvenliğinin korunması veya bu maddede belirtilenlere ilişkin kurallara uyum sağlanması da dâhil olmak üzere, yasal yükümlülüklerin, yargı organlarının veya yetkili idari kuruluşların talep veya gerekliliklerin yerine getirilmesi,
- Verilerin, gerekli güvenlik ve hukuki önlemler alınarak burada bahsedilen amaçların gerçekleştirilmesi için bilgi işlem altyapılarına, elektronik veya fiziki ortamlarda yasal yükümlülüklerin yerine getirilmesi amacıyla arşivlenmesi,
- Listeleme, raporlama, doğrulama, analiz ve değerlendirmeler yapmak, İstatistikî ve bilimsel bilgilerin üretilmesi,
- İlişkide bulunulan kişilerin internet sitesi, web uygulamaları, mobil uygulamalar ve diğer iletişim kanallarını, kullanım şekillerine ilişkin analiz yapması ve özelleştirmele rde bulunulması,
- Üniversite'nin ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Üniversite tarafından yürütülen finans operasyonları, iletişim, pazar araştırmaları ve sosyal sorumluluk aktiviteleri ile talep, teklif, değerlendirme, sipariş, bütçe, sözleşme gibi satın alma operasyonlarının yürütülmesi,
- Üniversite içi sistem ve uygulama yönetimi operasyonları ile hukuki operasyonların yönetilmesi,
- Üniversite ile ilişkisi bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) Üniversitemiz ve/veya Üniversitemize bağlı merkez ve birimlerinin ürün ve hizmetlerinden yararlanabilmeleri için gerekli çalışmaların ilgili birimleri tarafından yapılabilmesi,
- Üniversite ana kampüsü ve/veya bağlı merkez ve birimlerinde bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) can ve mal güvenlikleri ile hukuki, ticari ve iş sağlığı güvenliklerinin temini,
- 2547 sayılı Yükseköğretim Kanunu, 4857 sayılı İş Kanunu, 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu, 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 3308 sayılı Mesleki Eğitim Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 213 sayılı Vergi Usul Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 3359 sayılı Sağlık Hizmetleri Temel Kanunu, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, Özel Hastaneler Yönetmeliği, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Korunması Yönetmeliği vb. ilgili tüm kanunlardan ve ikincil düzenlemelerden doğan/doğabilecek yasal ve düzenleyici gereksinimlerin yerine getirilmesi ve bu kapsamda gerekli tedbirlerin alınabilmesi,

- Üniversitemizin ve Üniversitemizle ilişki içerisinde olan üçüncü, gerçek veya tüzel kişilerin hukuki ve ticari güvenliğinin temini ve bunlarla yapılan sözleşmeler veya yürütülen faaliyetler çerçevesinde, hukuki ve ticari yükümlülüklerin gerçekleştirilmesi,
- Üniversite tarafından iş ortağı, müşteri, tedarikçiler ve çalışanlarla yapılan sözleşmelerden kaynaklanan yükümlülüklerin ifası, hak tesisi, hakların korunması, ticari ve hukuki değerlendirme süreçleri, hukuki ve ticari risk analizleri, hukuki uyum süreci, mali işlerin yürütülmesi,
- Görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca yapılacak denetleme ve/veya düzenleme görevlerinin yürütülmesi,
- Öğrenciler ile akademik ve idari personel hakkında açılan/açılabilecek disiplin soruşturması süreçlerinin yönetilebilmesi,
- Üniversite bünyesinde bulunan öğrenci kulüplerine üye olunabilmesi, kulüp çatısı altında yapılan çalışmalardan, etkinliklerden ve organizasyonlardan yararlanılabilmesi; ayrıca dernek, vakıf, sivil toplum kuruluşu ve/veya sendikalarla herhangi bir işbirliği ve/veya bağlantısı bulunan bir kulübe üye olunması halinde, bu üyelik ile ilgili kanunlarda öngörülen kayıtların tutulabilmesi,
- Yargı organlarının ve/veya idari makamların istediği bilgi ve belge taleplerinin yerine getirilmesi,
- Üniversite ve Üniversiteye bağlı tüm merkez ve birimlerde sunulan ürün ve hizmetlerin kullanım şekline ilişkin listeleme, raporlama, doğrulama analiz çalışması yapmak, bu hususta istatistiki ve bilimsel bilgiler üretmek, buna bağlı olarak ürün ve hizmetlerimizi geliştirmek, ürün ve hizmetlerimize ilişkin memnuniyeti arttırmak ve bu kapsamda kullanıcıya ilişkin özelleştirmelerde bulunulması,
- Akademik eğitimler, bilimsel araştırmalar, proje başvuruları, Fikri ve Sınai Mülkiyet Kanunu kapsamındaki haklara ilişkin başvuru, devir vb. her türlü işlemler ile yayın, danışmanlık vb. her türlü faaliyetin sürdürülebilmesi,
- Üniversite ile Üniversiteye bağlı merkez ve birimlerin akreditasyon ve değerlendirme çalışmalarının yapılabilmesi,
- Kamu düzeninin ve sağlığının korunması,
- Koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım, medikal malzemelerinin temini gibi sağlık hizmetlerinin yürütülmesi ve yönetilmesi,
- Sunulan tüm hizmetlerin finansmanının planlanması ve yönetimi, faturalandırılmasının yapılması,
- Tüm çalışanların eğitilmesi ve geliştirilmesi,
- Eğitim, seminer vb. organizasyonlara katılım taleplerinin yerine getirilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Anlaşmalı olunan özel sigorta şirketleri ve/veya diğer kurumlar tarafından, anlaşmalar çerçevesinde sunulan teklif, promosyon, muafiyet vb. hak ve yükümlülüklerin yerine getirilmesi.

3. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR:

3.1. Kişisel Verilerin Güvenliğinin Sağlanması:

Üniversitemiz, Kanun'un 12. maddesine uygun olarak, kişisel verilerin hukuka aykırı olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerde meydana gelebilecek güvenlik eksikliklerini önlemek için, korunacak verinin niteliğine göre gerekli tedbirlerini almaktadır. Bu kapsamda Üniversitemiz, Kişisel Verileri Koruma Kurulu ("Kurul") tarafından yayımlanmış olan rehberlere uygun olarak gerekli güvenlik düzeyini sağlamaya yönelik ve idari tedbirleri almakta, denetimleri yapmakta veya yaptırmaktadır.

Tüm personel, Üniversite tarafından işlenen ve kendi sorumluluklarında olan kişisel verilerin güvenli olarak tutulmasını sağlamakla yükümlüdür. Kişisel verilere, yalnızca bunlara erişimi gerekli olanlar erişebilmelidir. Kişisel verilere ilişkin bilgi güvenliği olayları KVK Komitesince en kısa süre içerisinde KVK Kuruluna ve ilgili kişiye bildirilir.

Tüm personel ve çalışanlar, Üniversite tarafından işlenen ve kendi sorumluluklarında olan verilerin güvenli olarak tutulmasını ve gizlilik sözleşmesi imzalamadıkça üçüncü tarafa açıklanmamasını sağlamakla yükümlüdür.

3.2. Özel Nitelikli Kişisel Verilerin Korunması

Kanun ile birtakım kişisel verilere hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski nedeniyle özel önem atfedilmiştir. Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Üniversitemiz tarafından, Kanun ile "özel nitelikli" olarak belirlenen ve hukuka uygun olarak işlenen özel nitelikli kişisel verilerin korunmasında hassasiyetle davranılmaktadır. Bu kapsamda, Üniversite tarafından, kişisel verilerin korunması için alınan teknik ve idari tedbirler, özel nitelikli kişisel veriler bakımından özenle uygulanmakta ve Üniversite bünyesinde gerekli denetimler sağlanmaktadır. Özel nitelikli kişisel verilerin işlenmesi ile ilgili ayrıntılı bilgiye bu Politika'nın 4.3. ("Özel Nitelikli Kişisel Verilerin İşlenmesi") bölümünde yer verilmiştir.

3.3. İş Birimlerinin Kişisel Verilerin Korunması ve İşlenmesi Konusunda Farkındalıklarının Arttırılması ve Denetimi

Üniversitemiz, kişisel verilerin hukuka aykırı olarak işlenmesini, kişisel verilere hukuka aykırı olarak erişilmesini önlemeye ve kişisel verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için iş birimlerine gerekli eğitimlerin düzenlenmesini sağlamaktadır. Üniversite çalışanlarının kişisel verilerin

korunması konusunda farkındalığının oluşması için gerekli sistemler kurulmakta, konuya ilişkin ihtiyaç duyulması halinde danışmanlar ile çalışmaktadır. Bu doğrultuda Üniversitemiz, ilgili eğitimlere, seminerlere ve bilgilendirme oturumlarına yapılan katılımları değerlendirmekte olup ilgili mevzuatın güncellenmesine paralel olarak eğitimlerini güncellemekte ve yenilemektedir.

4.BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR

Üniversitemiz bakımından öncelikle önem arz eden hususlardan biri, kişisel verilerin işlenmesinde mevzuatta öngörülen genel ilkelere uygun davranılmasıdır. Bu kapsamda, Üniversite, Anayasa ve KVK Kanunu'na uygun olarak kişisel verilerin işlenmesinde aşağıda sıralanan ilkelere uygun hareket etmektedir.

4.1. Kişisel Verilerin Mevzuatta Öngörülen İlkelere Uygun Olarak İşlenmesi

4.1.1.Hukuka ve Dürüstlük Kuralına Uygun Kişisel Veri İşleme Faaliyetlerinde Bulunma

Üniversite, KVK Kanunu'nun 4. maddesine uygun olarak, kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmaktadır.

Bu kapsamda Üniversite, kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta ve kişisel verileri amacın gerektirdiği durumlar dışında kullanmamaktadır.

4.1.2. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama

İşlenen verilerin doğru ve güncel olmasını sağlamak için veri işleme prosedürlerinde gerekli tedbirler alınmakta, İlgili Kişiye verilerini güncellemesi ve var ise işlenen verilerindeki hataların düzeltilebilmesi için başvuru imkanı sunulmaktadır.

4.1.3. Belirli, Açık ve Meşru Amaçlarla İşleme

Kişisel veriler açık ve kesin olarak belirlenen amaçlarla bağlantılı, sınırlı ve ölçülü olarak işlenmektedir. İlgili olmayan veya işlenmesine ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmaktadır. Bu nedenle, yasal gereklilik olmadığı sürece özel nitelikte kişisel verileri işlememekte veya işlememiz gerektiğinde konuya ilişkin aydınlatmalar yapılarak açık rızalar alınmaktadır.

4.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel veriler açık ve kesin olarak belirlenen amaçlarla bağlantılı, sınırlı ve ölçülü olarak işlenmektedir. İlgili olmayan veya işlenmesine ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmaktadır. Bu nedenle, yasal gereklilik olmadığı sürece özel nitelikte kişisel verileri işlememekte veya işlememiz gerektiğinde konuya ilişkin aydınlatmalar yapılarak açık rızalar alınmaktadır.

4.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Etme

Üniversite, Türk Ceza Kanunu'nun 138.maddesine ve KVK Kanunu'nun 4. ve 7. maddelerine uygun olarak; işlediği kişisel verileri, yalnızca ilgili mevzuat ve kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar muhafaza etmektedir.

Bu kapsamda, Üniversite öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmaktadır. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Kişisel veriler

belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya İlgili Kişi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

Detaylar, Kişisel Verileri Saklama ve İmha Politikası'nda belirtilmiştir.

4.2.Kişisel Verilerin İşlenme Şartları

Kişisel veri sahibinin açık rıza vermesi haricinde kişisel veri işleme faaliyetinin dayanağı aşağıda belirtilen şartlardan yalnızca biri olabileceği gibi birden fazla şart da aynı kişisel veri işleme faaliyetinin dayanağı olabilmektedir. İşlenen verilerin özel nitelikli kişisel veri olması halinde, işbu Politika'nın 4.3 başlığı ("Özel Nitelikli Kişisel Verilerin İşlenmesi") içerisinde yer alan şartlar uygulanacaktır.

İ. Kanunlarda Açıkça Öngörülmesi

İlgili Kişinin kişisel verileri, kanunda açıkça öngörülmekte ise diğer bir ifade ile ilgili kanunda kişisel verilerin işlenmesine ilişkin açıkça bir hüküm olması halinde işbu veri işleme şartının varlığından söz edilebilecektir.

ii. Fiili İmkânsızlık Sebebiyle İlgilinin Açık Rızasının Alınamaması

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınamayacak olan kişinin kendisinin ya da başka bir kişinin hayatı veya beden bütünlüğünü korumak için kişisel verisinin işlenmesinin zorunlu olması halinde İlgili Kişinin kişisel verileri işlenebilecektir.

iii. Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması

İlgili Kişinin taraf olduğu bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, kişisel verilerin işlenmesinin gerekli olması halinde işbu şart yerine getirilmiş sayılabilecektir.

İV. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi

Üniversite'nin hukuki yükümlülüklerini yerine getirmesi için işlemenin zorunlu olması halinde, İlgili Kişinin kişisel verileri işlenebilecektir.

V. Kişisel İlgili Kişinin Kişisel Verisini Alenileştirmesi

İlgili Kişinin, kişisel verisini alenileştirmiş olması halinde ilgili kişisel veriler alenileştirme amacıyla sınırlı olarak işlenebilecektir.

Vİ. Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde İlgili Kişinin kişisel verileri işlenebilecektir.

Vİİ. Veri Sorumlusunun Meşru Menfaati için Veri İşlemenin Zorunlu Olması

İlgili Kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Üniversite'nin meşru menfaatleri için veri işlemesinin zorunlu olması halinde İlgili Kişinin kişisel verileri işlenebilecektir.

4.3-Özel Nitelikli Kişisel Verilerin İşlenmesi

İlgili Kişi açısından korunmasının çeşitli açılardan daha kritik önem teşkil ettiğine inanılan özel nitelikli kişisel verilerin işlenmesinde ise Üniversite tarafından özel hassasiyet gösterilmektedir. Özel nitelikli kişisel veriler Üniversitemiz tarafından, işbu Politika'da belirtilen ilkelere uygun olarak ve Kurul'un

belirleyeceği yöntemler de dahil olmak üzere gerekli her türlü idari ve teknik tedbirler alınarak ve aşağıdaki şartların varlığı halinde işlenmektedir:

(i) Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmesi diğer bir ifade ile ilgili faaliyetin tabi olduğu kanunda kişisel verilerin işlenmesine ilişkin açıkça bir hüküm olması halinde veri sahibinin açık rızası aranmaksızın işlenebilecektir. Aksi durumda söz konusu özel nitelikli kişisel verilerin işlenebilmesi için veri sahibinin açık rızası alınacaktır.

(ii) Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, 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 kuruluşlar tarafından açık rıza aranmaksızın işlenebilecektir. Aksi durumda söz konusu özel nitelikli kişisel verilerin işlenebilmesi için veri sahibinin açık rızası alınacaktır.

4.3.1 Özel Nitelikli Kişisel Verilerin Korunmasına İlişkin Önlemler

Üniversite, Kanun'un 6. Maddesinde yer alan, Özel Nitelikli Kişisel Veriler'in işlenmesinde, Kurul'un 31.01.2018 Tarihli ve 2018/10 Numaralı kararı uyarınca, veri sorumlusu sıfatıyla, aşağıda belirtilen önlemleri almaktadır:

A-Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika belirlenmiştir,

B-Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan Çalışan'lara yönelik;

- Kanun ve buna bağlı yönetmelikler ile Özel Nitelikli Kişisel Veri güvenliği konularında düzenli olarak eğitimler verilmektedir,
- Gizlilik sözleşmelerinin yapılmaktadır,
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamları ve süreleri net olarak tanımlanmaktadır,
- Periyodik olarak yetki kontrolleri gerçekleştirilmektedir,
- Görev değişikliği olan ya da işten ayrılan Çalışanlar'ın bu alandaki yetkileri derhal kaldırılmaktadır. Bu kapsamda, Veri Sorumlusu tarafından kendisine tahsis edilen envanteri iade almaktadır

C-Özel Nitelikli Kişisel Verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise,

- Kişisel Veriler, kriptografik yöntemler kullanılarak muhafaza edilmektedir,
- Kişisel Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanmaktadır,

D-Özel Nitelikli Kişisel Verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;

- Özel Nitelikli Kişisel Veriler'in bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmaktadır, Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

E-Özel Nitelikli Kişisel Veriler aktarılacaksa,

- Kişisel Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmaktadır,
- Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır,
- Kişisel Veriler'in kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "Gizli " formatta gönderilmektedir.

Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmaktadır.

4.4. Kişisel Veri Sahibinin Aydınlatılması

Üniversite, Kanun'un 10. maddesine ve ikincil mevzuata uygun olarak, kişisel veri sahiplerini aydınlatmaktadır. Bu kapsamda Üniversite, kişisel verilerin veri sorumlusu olarak kim tarafından, hangi amaçlarla işlendiği, hangi amaçlarla kimlerle paylaşıldığı, hangi yöntemlerle toplandığı ve hukuki sebebi ve veri sahiplerinin kişisel verilerinin işlenmesi kapsamında sahip olduğu hakları konusunda ilgili kişileri bilgilendirmektedir.

4.5.Kişisel Verilerin Aktarılması

Üniversite tarafından kişisel verilerin aktarılması konusunda KVKK'da öngörülen ve KVK Kurulu tarafından alınan karar ve düzenlemelere uygun bir şekilde hareket edilmektedir. Üniversitemiz hukuka uygun olan kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak İlgili Kişinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere (resmi ve özel mercilere, üçüncü gerçek kişilere) aktarabilmektedir. Üniversite bu doğrultuda Kanun'un 8. maddesinde öngörülen düzenlemelere uygun hareket etmektedir. Kişisel verilerin paylaşıldığı/paylaşılabileceği kişi gruplarının söz konusu olması durumunda ilgili kişiye aydınlatma metni ile bilgilendirme yapılmaktadır.

4.5.1 Kişisel Verilerin Aktarılması

Üniversitemiz, kişisel verilerin üçüncü taraflarla paylaşılması hususunda, diğer kanunlarda yer alan hükümler saklı kalmak kaydıyla, KVKK'da düzenlenen şartlara özenle uymaktadır. Bu çerçevede, kişisel veriler, veri sahibinin açık rızası olmadan üçüncü kişilere aktarılmamaktadır. Ancak, KVKK tarafından düzenlenen aşağıdaki şartlardan birinin varlığı halinde kişisel veriler; veri sahibinin açık rızası temin edilmeksizin de aktarılabilecektir:

- Kanunlarda açıkça öngörülmesi,

- 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,

- Bir 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,

- Veri sahibinin kendisi tarafından alenileştirilmiş olması,

- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- Veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Yukarıdakilere ek olarak kişisel veriler, Kurul tarafından yeterli korumaya sahip olduğu ilan edilen yabancı ülkelere **("Yeterli Korumaya Sahip Yabancı Ülke")** yukarıdaki şartlardan herhangi birinin varlığı halinde aktarılabilecektir.

Yeterli korumanın bulunmaması durumunda ise mevzuatta öngörülen veri aktarım şartları doğrultusunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ettiği ve Kurul'un izninin bulunduğu yabancı ülkelere **("Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülke")** aktarılabilecektir.

4.5.2.Özel Nitelikli Kişisel Verilerin Aktarılması:

Üniversitemiz, hukuka uygun olarak elde etmiş olduğu özel nitelikli kişisel verileri, veri işleme amaçları doğrultusunda, gerekli idari ve teknik tedbirleri alarak, İlgili Kişinin Özel Nitelikli Kişisel Verilerini üçüncü kişilere aktarabilmektedir. Üniversite, bu doğrultuda, özel nitelikli kişisel verileri, yukarıdaki bölümde belirtilen işleme şartlarından ve aşağıda yer alan şartlardan birinin varlığı halinde üçüncü kişilere aktarabilecektir.

(i) Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmesi diğer bir ifade ile ilgili kanunda kişisel verilerin işlenmesine ilişkin açıkça bir hüküm olması halinde veri sahibinin açık rıza aranmaksızın işlenebilecektir. Aksi halde veri sahibinin açık rızası alınacaktır.

(ii) Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, 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 kuruluşlar tarafından açık rıza aranmaksızın işlenebilecektir. Aksi halde veri sahibinin açık rızası alınacaktır.

Yukarıdakilere ek olarak kişisel veriler, **Yeterli Korumaya Sahip Yabancı Ülkelere** yukarıdaki şartlardan herhangi birinin varlığı halinde aktarılabilecektir. Yeterli korumanın bulunmaması durumunda ise mevzuatta öngörülen veri aktarım şartları doğrultusunda **Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülkelere** aktarılabilecektir.

5.BÖLÜM

KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

Üniversitemiz, kişisel verileri işlendikleri amaç için gerekli olan süre ve ilgili faaliyetin tabi olduğu yasal mevzuatta öngörülen minimum sürelere uygun olarak muhafaza etmektedir. Bu kapsamda, Üniversitemiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmaktadır. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır. Kişisel

veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Şartları:

Türk Ceza Kanunu'nun 138. maddesi, KVK Kanunu'nun 7. maddesi ve "Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Hakkında Yönetmelik" uyarınca, ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Üniversite'nin kendi kararına istinaden veya ilgili kişinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir. Üniversitece bu konuda yönetmelik hükümlerine göre bir politika oluşturmuş olup, bu politika uyarınca verinin niteliğine göre imha işlemi yapılmaktadır. Bu yönetmelik uyarınca Üniversite tarafından periyodik imha tarihleri belirlenmiş olup, yükümlülüğün başlaması ile beraber çeşitli aralıklarla periyodik imhanın yapılacağına göre takvim oluşturulmuştur.

Üniversite tarafından sıklıkla kullanılan anonimleştirme teknikleri aşağıda sıralanmaktadır.

Maskeleme

Veri maskeleme ile 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 vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkânsız hale geldiği bir veri setine dönüştürülmesi.

Toplulaştırma

Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

Veri Türetme

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 bölgenin belirtilmesi.

Veri Karma

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 hale getirilmesi.

6. BÖLÜM

KİŞİSEL VERİ SAHİPLERİNİN HAKLARI VE BU HAKLARIN KULLANILMASI

6.1. Kişisel Veri Sahibinin Hakları

Aydınlatma yükümlülüğü kapsamında, Üniversite tarafından İlgili Kişi bilgilendirilmekte ve bu bilgilendirmeye ilişkin sistem ve altyapılar kurulmaktadır. İlgili Kişinin kişisel verilerine ilişkin haklarını kullanması için gerekli olan teknik ve idari düzenlemeler Üniversitemiz tarafından yapılmaktadır.

İlgili Kişi kişisel verileri üzerinde;

- Kişisel verilerin işlenip işlenmediğini öğrenme,
- Kişisel veriler işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,
- Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- Yukarıda bahsedilen düzeltme, silme veya yok etme işlemlerinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhe bir sonuç ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme, haklarına sahiptir.

6.2. Kişisel Veri Sahibinin Haklarını Kullanması

İlgili Kişiler, yukarıda sayılan haklarını, www.agri.edu.tr adresinde yer alan İlgili Kişi başvuru formu vasıtasıyla ileterek kullanabilirler. Formun doldurulması yahut Üniversite'ye gönderilmesi hakkında detaylı bilgiler bu formda yer almaktadır.

6.3. Üniversitemizin Başvurulara Cevap Vermesi

Üniversitemiz, kişisel veri sahibi tarafından yapılacak başvuruları Kanun ve ikincil mevzuata uygun olarak sonuçlandırmak üzere gerekli idari ve teknik tedbirleri almaktadır. Kişisel veri sahibinin, bölüm 6.1.'de ("Kişisel Veri Sahibinin Hakları") yer alan haklara ilişkin talebini usule uygun olarak Üniversitemize iletmesi durumunda, Üniversitemiz talebin niteliğine göre en kısa sürede ve en geç 30 (otuz) gün içinde ilgili talebi ücretsiz olarak sonuçlandıracaktır. Ancak, işlemin ayrıca bir maliyet gerektirmesi halinde, Kurul tarafından belirlenen tarife uyarınca ücret alınabilecektir.

6.4. İlgili Kişinin Haklarını İleri Süremeyeceği Haller

KVKK'nın 28/2 hükmü uyarınca, aşağıdaki hallerde zararın giderilmesini talep etme hakkı hariç olmak üzere, ilgili kişilerin Kanun'un 11. maddesinde belirtilen haklardan yararlanmaları mümkün olmayacaktır;

- Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

- Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

7.BÖLÜM

KİŞİSEL VERİLERİN İŞLENDİĞİ ÖZEL DURUMLAR

7.1. Üniversite Bina, Tesis Girişlerinde ve İçerisinde Yürütülen Kamera ile İzleme Faaliyetleri

Üniversite tarafından bina ve tesislerinde güvenliğin sağlanması amacıyla Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata uygun olarak kamera ile izleme faaliyeti yürütülmektedir. Üniversite, bina ve tesislerinde güvenliğin sağlanması amacıyla, yürürlükte bulunan ilgili mevzuatta öngörülen amaçlarla ve Kanun'da sayılan kişisel veri işleme şartlarına uygun olarak güvenlik kamerası izleme faaliyetinde bulunmaktadır.

Üniversite tarafından Kanun'un 10. maddesine uygun olarak, kamera ile izleme faaliyetine ilişkin birden fazla yöntem ile kişisel veri sahibi aydınlatılmaktadır. Ayrıca, Üniversite, Kanun'un 4. maddesine uygun olarak, kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işlemektedir.

Üniversite tarafından video kamera ile izleme faaliyetinin sürdürülmesindeki amaç işbu Politika'da sayılan amaçlarla sınırlıdır. Bu doğrultuda, güvenlik kameralarının izleme alanları, sayısı ve ne zaman izleme yapılacağı, güvenlik amacına ulaşmak için yeterli ve bu amaçla sınırlı olarak uygulamaya alınmaktadır. Canlı kamera görüntüleri ile dijital ortamda kaydedilen ve muhafaza edilen kayıtlara yalnızca sınırlı sayıda çalışanının erişimi bulunmaktadır.

7.2.Üniversite Bina, Tesis Girişlerinde ve İçerisinde Yürütülen Misafir Giriş Çıkışlarının Takibi

Üniversite tarafından, güvenliğin sağlanması ve işbu Politika'da belirtilen amaçlarla, Üniversite binalarında ve tesislerinde ilgililerin giriş çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunulmaktadır. Misafir olarak Üniversite binalarına gelen kişilerin isim ve soyadları elde edilirken ya da Üniversite nezdinde asılan ya da diğer şekillerde misafirlerin erişimine sunulan metinler aracılığıyla söz konusu kişisel veri sahipleri bu kapsamda aydınlatılmaktadırlar.

Misafir giriş-çıkış takibi yapılması amacıyla elde edilen veriler yalnızca bu amaçla işlenmekte ve ilgili kişisel veriler fiziki ortamda veri kayıt sistemine kaydedilmektedir.

7.3.Ziyaretçilere Sağlanan İnternet Erişimleri

Üniversite tarafından güvenliğin sağlanması ve yürürlükte bulunan ilgili mevzuatta ve bu politikada belirtilen amaçlarla; Üniversite bina ve tesisleri içerisinde kalınan süre boyunca internet erişimi talep eden ziyaretçilere/misafirlere internet erişimi sağlanabilmektedir. Bu durumda internet erişimlerine ilişkin log kayıtları 5651 Sayılı Kanun ve bu Kanuna göre düzenlenmiş olan mevzuatın amir hükümlerine göre kayıt altına alınmakta; bu kayıtlar ancak yetkili kamu kurum ve kuruluşları tarafından talep

edilmesi veya Üniversite içinde gerçekleştirilecek denetim süreçlerinde ilgili hukuki yükümlülükleri yerine getirmek amacıyla işlenmektedir.

Bu çerçevede elde edilen log kayıtlarına yalnızca sınırlı sayıda Üniversite çalışanının erişimi bulunmaktadır. Bahsi geçen kayıtlara erişimi olan Üniversite çalışanları bu kayıtları yalnızca yetkili kamu kurum ve kuruluşundan gelen talep veya denetim süreçlerinde kullanmak üzere erişmekte ve hukuken yetkili olan kişilerle paylaşmaktadır. Kayıtlara erişimi olan sınırlı sayıda kişi iş sözleşmeleri ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

7.4.İnternet Sitesi Ziyaretçileri

Çerez kayıtları, Üniversite resmi internet sitesinin işleyiş biçimini ve kullanımını geliştirmeye yönelik olarak kullanılmaktadır. Üniversite resmi internet sitesinde geçirilen vaktin daha verimli ve keyifli hale getirilmesi amaçlanmaktadır. Bunların yanında, internet sitesinde yapılan tercihlerin hatırlanmasına yönelik bazı çerezlerden yararlanılmakta ve bu sayede kullanıcılara geliştirilmiş ve kişiselleştirilmiş bir deneyim sağlanmaktadır. İnternet sitesinde yer alan çerezler üzerinden kişisel veriler toplanmakta, toplanan veriler işlenmekte, aktarılmakta ve saklanabilmektedir. İnternet sitesinde kullanılan çerezlere ilişkin detaylı bilgi için "www.agri.edu.tr" resmi internet sitesinde yer alan " Çerez ve Gizlilik Politikasını" inceleyebilirsiniz.

8.BÖLÜM

KİŞİSEL VERİ İŞLEME FAALİYETİNE İLİŞKİN YÜKÜMLÜLÜKLER

Üniversitemiz, KVK Kanunu'nun veri sorumluları için öngördüğü yükümlülüklere uymalıdır. Bu kapsamda uymakla yükümlü olduğumuz başlıca hususlar aşağıda sıralanmaktadır:

8.1. Veri Sorumluları Siciline Kayıt ve Bildirim Yükümlülüğü

Üniversitemiz, KVK Kanunu'nun 16. maddesine ve Veri Sorumluları Sicili Hakkında Yönetmelik usul ve esaslarına uygun olarak, Veri Sorumluları Sicili'ne kaydolmakla yükümlü olup söz konusu yükümlülük Üniversitemizce yerine getirilmiştir.

8.2. Veri Sahibini Aydınlatma Yükümlülüğü

Üniversitemizce kişisel veriler toplanırken; öncelikle KVKK'nın 10. maddesine ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun olarak ilgili kişiler açıkça bilgilendirilerek aydınlatılmaktadır. Aydınlatma metinlerimizde;

- Üniversite'nin adı, açık adresi ve iletişim bilgileri,
- Kişisel veri kategorileri,
- Kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Verileri toplama yöntemi ve hukuki sebebi,
- İlgili kişinin KVKK'nın 11. maddesinde sayılan hakları, şeklinde alt başlıklar ve içerikleri yer almaktadır. Aydınlatma metnimizde yukarıda yer alan bilgilerin dışında başvuru yöntemleri de

sayılmıştır. Bu yöntemler sayesinde Kişisel Verilerin Korunmasında şeffaf ve ulaşılabilir olunması hedeflenmiştir.

Kamuoyuna açık olan işbu Politika'nın açık, anlaşılır, kolay erişebilir olmasına özen gösterilmektedir.

Ayrıca, çalışanlar, çalışan adayları, ziyaretçiler, vatandaşlar ve kamera sistemleri için Kişisel Verilerin Korunması Kanunu hakkındaki "Aydınlatma Metinlerini" Üniversite'nin internet sitesi üzerinden incelenebilecektir.

8.3. Kişisel Verilerin Güvenliğini Sağlama Yükümlülüğü

Üniversite, KVK Kanunu'nun 12. maddesine uygun olarak, kişisel verilerin güvenliğinin sağlanmasının ve veri sahiplerinin temel hak ve özgürlüklerinin gözetilmesinin öneminin bilinciyle;

1. Kişisel verilerin hukuka aykırı işlenmesini önlemek,

2. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve

3. Kişisel verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Üniversite bünyesinde, her açıdan güvenliğin sağlanmasının teşkil ettiği önemin bilinciyle, Üniversite, KVK Kanunu'nun 12. Maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verileri hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri alınmakta, bu kapsamda gerekli denetimler yapılmaktadır.

Üniversite, kişisel verilerin hukuka uygun işlenmesini sağlamak için, teknolojik imkanlar dahilinde, gerekli teknik ve idari tedbirleri almaktadır. Bu kapsamda Üniversitemizce alınan tedbirler aşağıda açıklandığı gibidir:

8.3.1. İdari Tedbirler

- Aydınlatma Metinleri (Çalışan, Çalışan Adayı, Müşteri, Kamera Sistemleri, Covid-19 Salgın Süreci) ve Açık Rıza Metinleri Hazırlanmıştır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim yetkileri düzenlenmiştir.
- Birim bazında kişisel verileri korumaya yönelik eğitim verilmiştir.
- Birim bazında belirlenen hukuksal uyum gerekliliklerinin sağlanması için ilgili birimin özelinde farkındalık yaratılmakta ve uygulama kuralları belirlenmekte; bu hususların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler hayata geçirilmektedir.
- Gizlilik taahhütnameleri yapılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin yönetmeliği hazırlanmıştır.

- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Katmanlı kamera aydınlatma metinleri kameraların bulunduğu bölgelere asılmıştır.
- Kişisel verilerin saklanması ile ilgili teknik ve idari riskler hakkında çalışanlar bilgilendirilerek farkındalık yaratılmıştır.
- Kurumun yürütmekte olduğu tüm faaliyetler detaylı olarak tüm birimlerin özelinde analiz edilerek, bu analiz neticesinde ilgili birimlerin gerçekleştirmiş olduğu faaliyetler özelinde kişisel veri işleme envanteri hazırlanmıştır.
- Kişisel Verileri Koruma Komitesi kurulmuştur.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- 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 mümkün olduğunca azaltılmaktadır.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Sözleşmeler KVKK İle uyumlu hale getirilmiştir.

8.3.2. Teknik Tedbirler

- Üniversite, veri güvenliğini sağlamak amacıyla bilgili ve deneyimli kişiler istihdam etmekte ve personeline gerekli kişisel verilerin korunmasına ilişkin eğitimleri vermektedir.
- Kurulan sistemler kapsamında gerekli iç kontrolleri yapılmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim yetkileri sınırlandırılmakta, yetkiler düzenli olarak gözden geçirilmektedir.
- Erişim logları düzenli olarak tutulmaktadır.
- Kişisel Verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte, Kişisel Verilerin bulunduğu veri depolama alanlarına erişimlerin iz kayıtları tutularak uygunsuz erişimler veya erişim denemeleri ilgililere iletilmektedir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.

- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

8.4. KVK Kurulu Tarafından Verilen Kararları Yerine Getirme Yükümlülüğü

Üniversite, kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak adına faaliyette bulunan ve KVK Kurumu'nun icra organı olan KVK Kurulu tarafından verilen kararlara uygun hareket etmektedir.

8.5. Veri Sahibi Başvurularına Cevap Verme Yükümlülüğü

Üniversite, veri sorumlusu sıfatıyla KVK Kanunu'nun 13. maddesi gereğince, veri sahiplerinin kişisel verilerine ilişkin taleplerini, talebin niteliğine göre en kısa sürede ve en geç otuz (30) gün içinde sonuçlandırmaktadır. Veri sahipleri kişisel verilerine ilişkin taleplerini Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ doğrultusunda gerçekleştirmelidir.

8.6. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Yükümlülüğü:

KVKK'nın 5 inci ve 6. maddelerinde yer alan 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. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesi zorunludur. Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür. Yukarıda belirtilen Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7. maddesi uyarınca Üniversite tarafından ayrıca Saklama ve İmha Politikası oluşturulmuştur.

9.BÖLÜM

9.1. KİŞİSEL VERİLERİ KORUMA KOMİSYONU

Üniversite bünyesinde, KVK Kanunu'na uygunluğun sağlanması, mevzuat düzenlemelerine uygun hareket edilmesi ve Kişisel Verilen Korunması ve İşlenmesi Politikasının yürürlüğünün ve sürdürülebilirliğinin sağlanması amacı ile üst yönetimin kararı ile Kişisel Verilerin Korunması Komisyonu oluşturulmuştur. Komisyonun görevleri aşağıda sıralanmıştır:

- Kişisel verilerin korunması ve işlenmesi ile ilgili temel politikaları ve gerektiğinde değişiklikleri hazırlamak ve yürürlüğe koymak amacı ile üst yönetiminin onayına sunmak.
- Kişisel verilerin korunması ve işlenmesine ilişkin politikaların uygulanması ve denetlenmesi ile ilgili faaliyetleri planlamak, bu çerçevede kurum içinde gerekli koordinasyonu sağlamak.
- KVK Kanunu ve ilgili mevzuata uyumun sağlanması için yapılması gereken faaliyetleri tespit etmek ve üst yönetimin onayına sunmak, onaylanan faaliyetlerin kurum içerisinde uygulanmasını gözetmek.
- Kişisel verilerin korunması ve işlenmesi konusunda Üniversite içerisinde ve Üniversite'nin iş birliği içerisinde olduğu kurumlar nezdinde farkındalığı arttırmak.
- Üniversite'nin kişisel veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini üst yönetimin onayına sunmak.
- Kişisel verilerin korunması ve işlenmesi ile ilgili politikaların uygulanması ve sürdürülmesi konusunda, kişisel veri sahiplerinin bilgilendirilmeleri amacı ile eğitim planlamaları yaparak üst yönetimin onayına sunmak.
- Kişisel veri sahiplerinin başvurularını en üst düzeyde karara bağlamak üzere üst yönetime iletmek.
- Kişisel verilerin korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak Üniversite içinde yapılması gerekenler konusundaki önerilerini üst yönetime iletmek.
- KVK Kurulu ve Kurumu ile olan ilişkileri koordine etmek ve komisyon başkanı nezdinde yürütmek.
- Üniversite üst yönetiminin kişisel verilerin korunması konusunda vereceği diğer görevleri yerine getirmek.

10. BÖLÜM

10.1.POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

Kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Üniversitemiz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir. Politika, ilgili mevzuat tarafından ortaya konulan kuralları Üniversite uygulamaları kapsamında somutlaştırılarak düzenlemektedir.

10.2. YETKİ VE SORUMLULUKLAR

Üniversite içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve diğer surette kurum nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her birimi 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 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.

Kişisel verilerin işlenmesi ve korunması süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Kişisel veri işleme ve koruma süreçleri görev dağılımı

ÜNVAN	BİRİM	GÖREV
REKTÖR	Ağrı İbrahim Çeçen Üniversitesi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
DEKAN	Fakülte	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
YÜKSEKOKUL VE ENSTİTÜ MÜDÜRÜ	Yüksekokul-Enstitü	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
GENEL SEKRETER	Genel Sekreterlik	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
DAİRE BAŞKANI	Daire Başkanlıkları	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
DİĞER YÖNETİCİLER	Rektörlüğe Bağlı Diğer Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
ÜNİVERSİTE KİŞİSEL VERİLERİ KORUMA KOMİSYONU	Ağrı İbrahim Çeçen Üniversitesi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi ile uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

10.3.POLİTİKA'NIN YÜRÜRLÜĞÜ

Politika, Ağrı İbrahim Çeçen Üniversitesi internet sitesinde (www.agri.edu.tr) yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

10.4.REVİZYON TABLOSU

Revizyon No	Revizyon Tarihi	Değişen Sayfa	Açıklama

AĞRI
İBRAHİM ÇEÇEN
ÜNİVERSİTESİ
2007

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1.BÖLÜM

1.1 GİRİŞ

Kişisel verilerin korunması, Ağrı İbrahim Çeçen Üniversitesi'nin ("Üniversite ") en önemli öncelikleri arasında olup, bu hususta yürürlükte bulunan tüm mevzuata uygun davranmak için azami gayret gösterilmektedir. İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika") ile Üniversitemizce işlenen kişisel verilerin teknik ve idari açıdan korunması, kişisel verilerin işlenme şartlarının ortadan kalkması halinde Kişisel Verilerin Korunması Kanunu ("Kanun") ile ilgili diğer yasal düzenlemelerde yer alan hükümlere uygun olarak imhası sağlanmaktadır.

1.2.AMAÇ

İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" ya da "Kanun") ve Kanun'un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerini silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla Üniversitemizce hazırlanmıştır.

1.3. KAPSAM

Üniversite'nin 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 kişilere ait kişisel veriler bu Politika kapsamında olup Üniversite'nin sahip olduğu ya da Üniversite tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde uygulanır.

2. BÖLÜM

2.1. TANIMLAR VE KISALTMALAR

ÜNİVERSİTE:	**Ağrı İbrahim Çeçen Üniversitesi**
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.

KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ELEKTRONİK ORTAM:	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
ELEKTRONİK OLMAYAN ORTAM:	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.
ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası
KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Üniversite Kişisel Veri Saklama ve İmha Politikası
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
İMHA:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
İLGİLİ KULLANICI:	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 kişiler.
İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişiler.
KAYIT ORTAMI:	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.
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
ÖĞRENCİ:	Kişisel verilerini eğitim maksadıyla Üniversitemizin incelemesine açmış olan gerçek kişiler
ÖĞRENCİ ADAYI:	Üniversitemize herhangi bir yolla ulaşmış, bilgilerini Üniversitemizin incelemesine açmış olan gerçek kişiler
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
YÖNETMELİK:	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.2.YETKİ VE SORUMLULUKLAR

Üniversitenin tüm birimleri ve çalışanları, işbu Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, 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 Kişisel Verileri Koruma Komisyonuna aktif olarak destek verir.

Kişisel Verileri Koruma Kurulu ile yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme ve sicile kayıt gibi işlemlerin sorumluluğu "Veri Sorumlusu İrtibat Kişi"sindedir.

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

Tablo 1: Kişisel veri saklama ve imha süreçleri görev dağılımı

ÜNVAN	BİRİM	GÖREV
REKTÖR	Ağrı İbrahim Çeçen Üniversitesi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
DEKAN	Fakülte	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
YÜKSEKOKUL VE ENSTİTÜ MÜDÜRÜ	Yüksekokul-Enstitü	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
GENEL SEKRETER	Genel Sekreterlik	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
DAİRE BAŞKANI	Daire Başkanlıkları	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
DİĞER YÖNETİCİLER	Rektörlüğe Bağlı Diğer Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
ÜNİVERSİTE KİŞİSEL VERİLERİ KORUMA KOMİSYONU	Ağrı İbrahim Çeçen Üniversitesi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi ile uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

2.3.KİŞİSEL VERİLERİN BULUNDUĞU ORTAMLAR

Kişisel veriler, Üniversitemiz tarafından aşağıda belirtilen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar

• Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) Yazılımlar (ofis yazılımları.) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.)	• Yazıcı, tarayıcı, fotokopi makinesi • Kağıt • Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) • Yazılı, basılı, görsel ortamlar • Birim dolapları

3. BÖLÜM

SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Üniversitemiz tarafından; Üniversite'nin idari yetkilileri, akademik ve idari personeli, öğrencileri, mezunları, personel adayları, öğrenci adayları, ziyaretçileri, iş birliği içinde olduğu kurumların çalışanları ve diğer üçüncü kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

3.1. SAKLAMAYA İLİŞKİN AÇIKLAMALAR

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.

3.1.1. 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,
- 2547 sayılı Yükseköğretim Kanunu,

- 3308 sayılı Mesleki Eğitim Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4734 sayılı Kamu İhale 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,
- 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
- Yüksek Öğrenim Kredi ve Yurtlar Kurumu Burs-Kredi Yönetmeliği
- Yükseköğretim Kurumları Bilimsel Araştırma Projeleri Hakkında Yönetmeliği
- Yükseköğretim Kalite Güvencesi ve Yükseköğretim Kalite Kurulu Yönetmeliği
- Yükseköğretim Kurumları Bilimsel Araştırma Projeleri Hakkında Yönetmelik
- Yükseköğretim Kurumları Döner Sermaye İşletmelerinin Kurulmasına İlişkin Yönetmelik
- Yükseköğretim Kurumları Kısmi Zamanlı Öğrenci Çalıştırma Usul ve Esasları Yükseköğretim Kurumlarında Uzaktan Öğretime İlişkin Usul ve Esaslar

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

3.1.2. Saklamayı Gerektiren İşleme Amaçları

Üniversitemiz faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklamaktadır:

- Üniversitemizin ortaya koymuş olduğu her türlü faaliyetten faydalananlar için gerekli çalışmaların, ilgili iş birimleri tarafından yapılması,
- Yükseköğretim Kanunu, ilgili ikincil düzenlemeler ve Yükseköğretim Kurumu (YÖK) tarafından getirilen eğitim faaliyetlerine ve denetime ilişkin ve sair yükümlülüklerin karşılanması,
- Eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık faaliyetlerinin sürdürülmesi, yükseköğretim mevzuatı ve Üniversitemiz iç düzenlemeleri kapsamında eğitim faaliyetinden kaynaklı hakların tesis edilmesi, kimlik kartı üretimi, basımı ile çeşitli akademik ve idari işlemlerin yapılması,
- Üniversitemizin stratejilerinin belirlenmesi ve uygulanması, Üniversitemizin ve faaliyetlerinin tanıtılması, Üniversitemizin insan kaynakları politikalarının yürütülmesi,

- İlgili bölümlerde eğitim gören ve Üniversite bünyesindeki birimlerde veya üniversite dışındaki kuruluşlarda staj yapan öğrencilerin hak ve yükümlülüklerinin korunması ve yerine getirilmesinin sağlanması,
- Üniversite öğrenci topluluklarından birisine üye olunması halinde, toplulukların bağlantıda olduğu dernek, vakıf, sivil toplum kuruluşları ile Üniversite tarafından Kanunlarda ön görülen kayıtların tutulması amacıyla işlenmesi, gerekli olması halinde kanunen yetkili kamu kurum, kuruluş ve özel kişilerle paylaşılması,
- Üniversite öğrencilerinin, çalışanlarının, ziyaretçilerinin can ve mal güvenliğinin korunması veya bu maddede belirtilenlere ilişkin kurallara uyum sağlanması da dâhil olmak üzere, yasal yükümlülüklerin, yargı organlarının veya yetkili idari kuruluşların talep veya gerekliliklerin yerine getirilmesi,
- Verilerin, gerekli güvenlik ve hukuki önlemler alınarak burada bahsedilen amaçların gerçekleştirilmesi için bilgi işlem altyapılarına, elektronik veya fiziki ortamlarda yasal yükümlülüklerin yerine getirilmesi amacıyla arşivlenmesi,
- Listeleme, raporlama, doğrulama, analiz ve değerlendirmeler yapmak, İstatistikî ve bilimsel bilgilerin üretilmesi,
- İlişkide bulunulan kişilerin internet sitesi, web uygulamaları, mobil uygulamalar ve diğer iletişim kanallarını, kullanım şekillerine ilişkin analiz yapması ve özelleştirmelerde bulunulması,
- Üniversite'nin ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Üniversite tarafından yürütülen finans operasyonları, iletişim, pazar araştırmaları ve sosyal sorumluluk aktiviteleri ile talep, teklif, değerlendirme, sipariş, bütçe, sözleşme gibi satın alma operasyonlarının yürütülmesi,
- Üniversite içi sistem ve uygulama yönetimi operasyonları ile hukuki operasyonların yönetilmesi,
- Üniversite ile ilişkisi bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) Üniversitemiz ve/veya Üniversitemize bağlı merkez ve birimlerinin ürün ve hizmetlerinden yararlanabilmeleri için gerekli çalışmaların ilgili birimleri tarafından yapılabilmesi,
- Üniversite ana kampüsü ve/veya bağlı merkez ve birimlerinde bulunan gerçek ve/veya tüzel üçüncü kişi kurum ve kuruluşların (öğrenciler, çalışanlar, ziyaretçiler, hastalar, tedarikçiler, iş ortakları vb.) can ve mal güvenlikleri ile hukuki, ticari ve iş sağlığı güvenliklerinin temini,
- 2547 sayılı Yükseköğretim Kanunu, 4857 sayılı İş Kanunu, 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu, 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 3308 sayılı Mesleki Eğitim Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 213 sayılı Vergi Usul Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 3359 sayılı Sağlık Hizmetleri Temel Kanunu, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, Özel Hastaneler Yönetmeliği, Kişisel Sağlık Verilerinin

İşlenmesi ve Mahremiyetinin Korunması Yönetmeliği vb. ilgili tüm kanunlardan ve ikincil düzenlemelerden doğan/doğabilecek yasal ve düzenleyici gereksinimlerin yerine getirilmesi ve bu kapsamda gerekli tedbirlerin alınabilmesi,

- Üniversitemizin ve Üniversitemizle ilişki içerisinde olan üçüncü, gerçek veya tüzel kişilerin hukuki ve ticari güvenliğinin temini ve bunlarla yapılan sözleşmeler veya yürütülen faaliyetler çerçevesinde, hukuki ve ticari yükümlülüklerin gerçekleştirilmesi,
- Üniversite tarafından iş ortağı, müşteri, tedarikçiler ve çalışanlarla yapılan sözleşmelerden kaynaklanan yükümlülüklerin ifası, hak tesisi, hakların korunması, ticari ve hukuki değerlendirme süreçleri, hukuki ve ticari risk analizleri, hukuki uyum süreci, mali işlerin yürütülmesi,
- Görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca yapılacak denetleme ve/veya düzenleme görevlerinin yürütülmesi,
- Öğrenciler ile akademik ve idari personel hakkında açılan/açılabilecek disiplin soruşturması süreçlerinin yönetilebilmesi,
- Üniversite bünyesinde bulunan öğrenci kulüplerine üye olunabilmesi, kulüp çatısı altında yapılan çalışmalardan, etkinliklerden ve organizasyonlardan yararlanılabilmesi; ayrıca dernek, vakıf, sivil toplum kuruluşu ve/veya sendikalarla herhangi bir işbirliği ve/veya bağlantısı bulunan bir kulübe üye olunması halinde, bu üyelik ile ilgili kanunlarda öngörülen kayıtların tutulabilmesi,
- Yargı organlarının ve/veya idari makamların istediği bilgi ve belge taleplerinin yerine getirilmesi,
- Üniversite ve Üniversiteye bağlı tüm merkez ve birimlerde sunulan ürün ve hizmetlerin kullanım şekline ilişkin listeleme, raporlama, doğrulama analiz çalışması yapmak, bu hususta istatistiki ve bilimsel bilgiler üretmek, buna bağlı olarak ürün ve hizmetlerimizi geliştirmek, ürün ve hizmetlerimize ilişkin memnuniyeti arttırmak ve bu kapsamda kullanıcıya ilişkin özelleştirmelerde bulunmak,
- Akademik eğitimler, bilimsel araştırmalar, proje başvuruları, Fikri ve Sınai Mülkiyet Kanunu kapsamındaki haklara ilişkin başvuru, devir vb. her türlü işlemler ile yayın, danışmanlık vb. her türlü faaliyetin sürdürülebilmesi,
- Üniversite ile Üniversiteye bağlı merkez ve birimlerin akreditasyon ve değerlendirme çalışmalarının yapılabilmesi,
- Kamu düzeninin ve sağlığının korunması,
- Koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım, medikal malzemelerinin temini gibi sağlık hizmetlerinin yürütülmesi ve yönetilmesi,
- Sunulan tüm hizmetlerin finansmanının planlanması ve yönetimi, faturalandırılmasının yapılması,
- Tüm çalışanların eğitilmesi ve geliştirilmesi,

- Eğitim, seminer vb. organizasyonlara katılım taleplerinin yerine getirilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Anlaşmalı olunan özel sigorta şirketleri ve/veya diğer kurumlar tarafından, anlaşmalar çerçevesinde sunulan teklif, promosyon, muafiyet vb. hak ve yükümlülüklerin yerine getirilmesi,
- Hukuki uyum süreçlerinin yürütülmesi,
- Operasyonların yönetimi,
- Mali ve finansal işlerin yerine getirilmesi,
- Ticari ve iş stratejilerinin belirlenmesi ve yerine getirilmesi,
- Hizmet sözleşmesine bağlı olarak; hizmet yükümlülüklerinin yerine getirilmesi,
- Acil durum yönetimi süreçlerinin yürütülmesi,
- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,
- Çalışanlar için yan haklar ve menfaatleri süreçlerinin yürütülmesi,,
- Çalışanlar için iş faaliyetlerinin yürütülmesi,
- Çalışanların başvuru süreçlerinin değerlendirilmesi,
- Faaliyetlerin mevzuata uygun yürütülmesi,
- İnsan kaynakları faaliyetinin planlanması,
- İş sağlığı / güvenliği faaliyetlerinin yürütülmesi,
- Yetkili kişi, kurum ve kuruluşlara haber verilmesi.

3.2. İMHAYI GEREKTİREN SEBEPLER

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- 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 Kurum tarafından kabul edilmesi,
- Üniversite'nin İlgili 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, Üniversitemiz tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER

Üniversitemiz, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmakta veya yaptırmaktadır. İşlenen kişisel verilerin teknik ve idari tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi durumunda, Üniversitemiz bu durumu mümkün olan en kısa süre içerisinde ilgili kişi ve birimlere haber vermektedir.

4.1 Teknik Tedbirler

Üniversitemizce teknik tedbirler kapsamında:

- Veri güvenliğini sağlamak amacıyla bilgili ve deneyimli kişiler istihdam etmekte ve personeline gerekli kişisel verilerin korunmasına ilişkin eğitimleri vermektedir.
- Kurulan sistemler kapsamında gerekli iç kontrolleri yapılmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim yetkileri sınırlandırılmakta, yetkiler düzenli olarak gözden geçirilmektedir.
- Erişim logları düzenli olarak tutulmaktadır.
- Kişisel Verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte, Kişisel Verilerin bulunduğu veri depolama alanlarına erişimlerin iz kayıtları tutularak uygunsuz erişimler veya erişim denemeleri ilgililere iletilmektedir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

4.2 İdari Tedbirler

Üniversitemiz tarafından, işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda belirtildiği gibidir:

- Aydınlatma Metinleri (Çalışan, Çalışan Adayı, Müşteri, Kamera Sistemleri, Covid-19 Salgın Süreci) ve Açık Rıza Metinleri Hazırlanmıştır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim yetkileri düzenlenmiştir.
- Birim bazında kişisel verileri korumaya yönelik eğitim verilmiştir.
- Birim bazında belirlenen hukuksal uyum gerekliliklerinin sağlanması için ilgili birimin özelinde farkındalık yaratılmakta ve uygulama kuralları belirlenmekte; bu hususların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler hayata geçirilmektedir.
- Gizlilik taahhütnameleri yapılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin yönetmeliği hazırlanmıştır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Katmanlı kamera aydınlatma metinleri kameraların bulunduğu bölgelere asılmıştır.
- Kişisel verilerin saklanması ile ilgili teknik ve idari riskler hakkında çalışanlar bilgilendirilerek farkındalık yaratılmıştır.
- Üniversite'nin yürütmekte olduğu tüm faaliyetler detaylı olarak tüm birimlerin özelinde analiz edilerek, bu analiz neticesinde ilgili birimlerin gerçekleştirmiş olduğu faaliyetler özelinde kişisel veri işleme envanteri hazırlanmıştır.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- 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 mümkün olduğunca azaltılmaktadır.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Sözleşmeler KVKK İle uyumlu hale getirilmiştir.

- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede ilgilisine ve Kurul'a bildirilmektedir.

5.BÖLÜM

KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Üniversitemiz tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilmektedir.

5.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Üniversitemiz kişisel verilerin silinmesi yöntemi olarak aşağıdaki yöntemlerden bir veya birkaçını kullanabilir:

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için 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.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

5.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin aşağıdaki yöntemlerle hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Üniversitemiz kişisel verilerin yok edilmesi yöntemi olarak aşağıdaki yöntemlerden bir veya birkaçını kullanabilir:

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

5.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

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 getirilmesi gerekir.

Üniversitemiz, kişisel verileri anonim hale getirmek için aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

Yöntem	Açıklama
Maskeleme (Masking)	Veri maskeleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir
Bölgesel Gizleme	Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.
Kayıtları Çıkartma	Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.

Global Kodlama	Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.
Gürültü Ekleme	Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

Üniversitemiz kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin re'sen karar alabilecek ve seçmiş olduğu kategoriye göre kullanacağı yöntemi de serbestçe belirleyebilecektir. Ayrıca Yönetmelik'in 13. maddesi kapsamında ilgili kişinin başvuru esnasında kendisine ait kişisel verinin silinmesi, yok edilmesi yahut anonim hale getirilmesi kategorilerinden birini seçmesi halinde de ilgili kategoride kullanılacak yöntemler konusunda Üniversitemiz serbesti içinde olacaktır.

6.BÖLÜM

SAKLAMA VE İMHA SÜRELERİ

Üniversite, 6698 sayılı KVK Kanunu ve diğer mevzuatta öngörülen saklama süreleri uyarınca saklanan kişisel verileri re'sen silme, yok etme veya anonim hale getirme işlemi yöntemlerinden biri ile imha eder.

Kişisel veri bazında saklama süreleri "Üniversite Kişisel Veri İşleme Envanteri Formu" ve veri kategorileri bazında VERBİS'te yer alır.

Üniversite, 6698 sayılı KVK Kanunu, mevzuat, "Kişisel Verilerin İşlenmesi ve Korunması Politikası" ve işbu politika uyarınca sorumlu olduğu 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. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 5 (Beş) yıl süreyle saklanır.

7.BÖLÜM

7.1.PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Üniversitemiz, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Üniversitemizde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

7.2. POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

Kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Üniversitemiz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir.

7.3. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

İşbu Politika'nın yürürlük tarihi 31.12.2021 dir. Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, Üniversite'nin internet sayfasında kamuya açıklanır.

7.4.POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

7.5.POLİTİKA'NIN YÜRÜRLÜĞÜ

Politika, Ağrı İbrahim Çeçen Üniversitesi internet sitesinde www.agri.edu.tr internet sitesinde yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

7.6.REVİZYON TABLOSU

Revizyon No	Revizyon Tarihi	Değişen Sayfa	Açıklama

AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ 2007

VERİ İHLALİ MÜDAHALE POLİTİKASI

logo

1.GİRİŞ

Kişisel verilerin korunması, Üniversitemizin en önemli öncelikleri arasında olup, bu hususta yürürlükte bulunan tüm mevzuata uygun davranmak için azami gayret gösterilmektedir. İşbu Veri İhlali Müdahale Politikası ("Politika") çerçevesinde Üniversitemiz tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin yürütülmesinde yaşanması muhtemel bir veri ihlalinde izlenmesi gereken prosedür ortaya konulmakta, böylelikle Üniversitemiz, kişisel veri sahiplerini bilgilendirerek gerekli şeffaflığı sağlamaktadır.

2.AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'ncimaddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri İhlali Müdahale Politikası ("Politika"), Üniversitemizce işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Üniversitemiz tarafından benimsenecek ve uygulamada dikkate alınacak faaliyetleri belirlemek amacıyla hazırlanmıştır.

3. KAPSAM

Politika hükümleri, Üniversitemizin faaliyet konuları ve çalışma alanlarında kişisel verilerin işlenmesi süreçlerine dahil olan tüm bilgi sistemlerini ve alt bilgileri, kontratları, çevre ve fiziksel alanları ve tüm bunlar için üretilen sistem ve düzenlemeleri kapsamaktadır. Bu politika Üniversite'nin tüm birimlerini, destek hizmeti veren firma personellerini, ziyaretçileri, üçüncü kişileri, stajyer ve sözleşmeli personeli kapsamaktadır.

4.SORUMLULUKLAR

Politika'nın Üniversitemizin işleyiş, faaliyet ve süreçlerinde ve uygulanmasında, hukuki yönden risklerin ve yakın tehlikenin önlenmesinde Üniversite genelinde tüm çalışanlarımız, paydaşlarımız, misafirler, ziyaretçiler ve ilgili üçüncü kişiler iş birliği yapmakla yükümlüdür. Üniversite'nin tüm organ ve departmanları Üniversite Veri İhlali Müdahale Politikası'nın uygulanmasından sorumludur.

5.VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

Kişisel Verilerin Korunması Kanunu'na göre kişisel veri güvenliğinin temini için Veri Sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

6. TANIMLAR VE KISALTMALAR

ÜNİVERSİTE:	Ağrı İbrahim Çeçen Üniversitesi
AÇIK RIZA:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
ANONİM HALE GETİRME:	Kişisel verinin, kişisel veri niteliği kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
İLGİLİ KİŞİ:	Kişisel verisi işlenen gerçek kişi. Ör: Müşteriler, ziyaretçiler, çalışanlar ve çalışan adayları.
KİŞİSEL VERİ:	Kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örn: ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası, banka hesap numarası vb.
ÖZEL NİTELİKLİ KİŞİSEL VERİ:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
KİŞİSEL VERİLERİN İŞLENMESİ:	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.
VERİ SORUMLUSU:	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten gerçek veya tüzel kişiyi ifade eder
VERİ SAHİBİ BAŞVURU FORMU:	İlgili Kişinin, KVK Kanunu'nun 11. maddesinde yer alan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.
ANAYASA:	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan;7 Kasım 1982 tarihli 2709 sayılı Türkiye Cumhuriyeti Anayasası

KVK KANUNU:	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
POLİTİKA:	Veri İhlali Müdahale Politikası
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ:	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI:	Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi Hakkında Yönetmelik gereğince, Üniversite tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika
PERİYODİK İMHA:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
KAYITLI ELEKTRONİK POSTA (KEP):	Her türlü ticari, hukuki yazışma ve belge paylaşımlarınızı gönderdiğiniz biçimde koruyan, alıcının kim olduğunu kesin olarak tespit eden, içeriğin kesinlikle değişmemesini ve içeriği yasal geçerli ve güvenli, kesin delil haline getiren sistemdir.
VERİ SORUMLULARI SİCİL BİLGİ SİSTEMİ:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

7.KİŞİSEL VERİ İHLALİ

Kişisel veri ihlali, kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, hukuka aykırı bir şekilde kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin yanlışlıkla/kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda ortaya çıkmaktadır.

Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak değerlendirilir:

- Kişisel veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi,
- Gizli bilgilerin hukuka aykırı şekilde ifşası,

- Kişisel veri ve/veya gizli bilgi içeren e-postaların yanlışlıkla Üniversite dışında ilgisiz kişilere iletilmesi, gönderimi,
- Üniversite ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı)gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

Yukarıda belirtilen veya benzer durumlarda bu Prosedür'de belirtilen şekilde hareket edilmelidir.

8.VERİ İHLALİ MÜDAHALE EKİBİ

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıdaki departmanlardan belirlenen katılımcıların dahil edileceği bir Kriz Müdahale Ekibi (Ekip) oluşturulur:

- Veri Sorumlusu İrtibat Kişisi
- Veri Sorumlusu Üst Yöneticisi (Genel Müdür)
- İhlalin Meydana Geldiği Departmanın Yöneticisi

9.VERİ İHLALİ MÜDAHALE SÜRECİ

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

Buna göre, İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde Üniversite, söz konusu veri ihlalini, en kısa sürede (en geç 72 saat) Kurul'a ve söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip makul olan en kısa süre içerisinde ilgili kişiye bildirmelidir.

İlgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Üniversite'nin kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmalıdır.

Veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak;

- İhlalinin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi gerekmektedir.

Kurula yapılacak bildirimde yine Kurul'un belirlediği ve web sitesinde yayınladığı KVK Kurulu Veri İhlal Bildirim Formu doldurularak Kurula iletilir.

Üniversite tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması gerekmektedir.

Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanmalıdır.

Üniversite tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması sağlanmalıdır.

Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin Üniversite'ye bildirimde bulunmalıdır.

Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmalıdır.

Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu plan gözden geçirilmelidir.

10.POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

Kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Üniversitemiz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir. Politika, ilgili mevzuat tarafından ortaya konulan kuralları Üniversite uygulamaları kapsamında somutlaştırılarak düzenlemektedir.

11. POLİTİKA'NIN YÜRÜRLÜĞÜ

İşbu Politika'nın yürürlük tarihi 31.12.2021'dir. İşbu Politika, Üniversitemizin internet sitesinde yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

12.DAĞITIM

Politika, Üniversite internet sitesinde yayınlanarak, Üniversite'nin 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 kişilere ve diğer üçüncü kişilere duyurulur.

13. REVİZYON TABLOSU

Revizyon No	Revizyon Tarihi	Değişen Sayfa	Açıklama