



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

AMAÇ

Bu politikanın amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK” veya “Kanun”) ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“Yönetmelik”) uyarınca yükümlülüklerimizi yerine getirmek, kişisel verilerin işlendikleri amaç için gerekli olan azami saklama ve imha sürelerini belirlemektir. Bu kapsamda öğrencilerimiz, mezunlarımız, çalışan adaylarımız, yetkililerimiz, ziyaretçilerimiz, işbirliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkilileri ve üçüncü kişiler başta olmak üzere kişisel verileri Üniversitemiz tarafından işlenen kişileri bilgilendirerek şeffaflığı sağlamaktır.

KAPSAM

Bu politika, öğrencilerimizin, mezunlarımızın, çalışan adaylarımızın, yetkililerimizin, ziyaretçilerimizin, işbirliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkililerinin ve üçüncü kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verilerine ilişkindir.

Yukarıda belirtilen kategorilerde yer alan kişisel veri sahipleri gruplarına ilişkin işbu politikanın uygulama kapsamı politikanın tamamı olabileceği gibi (örn. ziyaretçimiz de olan mezunlarımız gibi); yalnızca bir kısım hükümleri de (örn. yalnızca ziyaretçilerimiz gibi) olabilecektir.

REFERANSLAR

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

SORUMLULUKLAR

- Bu dokümanın uygulanmasından Rektör sorumludur.
- Bu politikanın hazırlanmasından ve güncellenmesinden Kişisel Verileri Koruma Komisyonu sorumludur.

TANIMLAR

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

Anonim hale getirme: Kişisel verinin, kişisel veri niteliğini kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleyme, toplulaştırma,

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.

İmha : Kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi.

Kayıt ortamı : Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yollardan işlenen kişisel verilerin bulunduğu her türlü ortamı,

Periyodik İmha : Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.

Silme : Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.

Yok Etme : Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesidir.

Yönetmelik : 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Çalışan : Marmara Üniversitesi çalışanları

İlgili Kişi Başvuru Formu : Kişisel veri sahiplerinin haklarını kullanmak için yapacakları başvuruyu içerecek, MÜ-KVKK-FR01 KVKK İlgili Kişi Başvuru Formu

Çalışan adayı : Üniversitemize herhangi bir yolla iş veya staj başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini Üniversitemizin incelemesine açmış olan gerçek kişiler

İşbirliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkilileri: Üniversitemizin her türlü iş ilişkisi içerisinde bulunduğu kurumlarda (iş ortağı, tedarikçi gibi, ancak bunlarla sınırlı olmaksızın) çalışan, bu kurumların hissedarları ve yetkilileri dâhil olmak üzere, gerçek kişiler

İş Ortağı : Üniversitemizin faaliyetlerini yürütürken iş ortaklığı kurduğu taraflar

Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem

Kişisel veri sahibi : Kişisel verisi işlenen gerçek kişi. Örneğin; öğrenciler, mezunlar.

Kişisel veri : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örneğin; ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası vb.

Özel nitelikli kişisel veri : 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

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

Üniversite yetkilisi : Üniversite rektörlük yetkilileri ile diğer yetkili gerçek kişiler

Tedarikçi : Üniversitemizin faaliyetlerini yürütürken Üniversitemizin emir ve talimatlarına uygun olarak sözleşme temelli olarak Üniversitemize hizmet sunan taraflar

Üçüncü kişi : Politika kapsamında farklı bir şekilde tanımlanmamış olan, kişisel verileri politika kapsamında işlenen gerçek kişiler (Örn. Kefil, refakatçi, aile bireyleri ve yakınlar)

Veri işleyen : Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi. Örneğin, KampüsKart firması v.b.

Veri sorumlusu : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten kişi

Ziyaretçi : Üniversitemizin sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan, etkinliklerimize katılan veya internet sitelerimizi ziyaret eden gerçek kişiler

KVK Kanunu / Kanun : 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete’de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu

AB : Avrupa Birliği

Anayasa: 9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete’de yayımlanan; 7 Kasım 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası.

KVK Kurulu : Kişisel Verileri Koruma Kurulu

KVK Kurumu : Kişisel Verileri Koruma Kurumu

Politika : MU-KVKK-PL01 Kişisel Verilerin Korunması İşlenmesi ve İmha Politikası

Üniversite/ Üniversitemiz : Marmara Üniversitesi

Türk Ceza Kanunu : 12 Ekim 2004 tarihli ve 25611 sayılı Resmi Gazete’de yayımlanan; 26 Eylül 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu.

KAYIT ORTAMLARI

Üniversite bünyesinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir şekilde aşağıdaki kayıt ortamlarında hassas bir şekilde muhafaza edilmektedir.

Elektronik ortamlar;

Ms Office Dosyaları

Sunucularımız

Antivirüs programları ve güvenlik duvarı ile hassas bir şekilde korunan bilgisayarlarımız

Ağ cihazlarımız

Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüler

Üniversitemize ait Bulut sistemleri,

Mobil telefonlar ve içerisindeki tüm saklama alanları,

Yazıcı, Parmak izi okuyucu gibi çevre birimler

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

Manyetik bantlar,
Optik diskler,
Flash hafızalar
File Server
DHCP
DC
SQL veri tabanı
MySQL veri tabanı

Fiziki ortamlar;

Birim Dolapları
Birim Arşivi
Kurum Arşivi
Arşiv
Muhasebe Birimi
Personel Birimi
Öğrenci İşleri Birimi

KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Üniversite bünyesinde bulunan kişisel veriler, Üniversitemizin hizmetlerinin sunulması, eğitim faaliyetlerinin kesintisiz olarak sürdürülmesi, hukuki yükümlülüklerinin yerine getirilmesi, çalışan haklarının planlanması ve yerine getirilmesi amacıyla; aşağıda yer alan veri işleme sebepleriyle İşbu Politika'da belirtilen elektronik ya da fiziki ortamlarda güvenli ve hassas bir şekilde saklanmakta ve yine bu sebeplerin ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine imha edilmektedir.

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

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

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

Üniversitemiz, kişisel verilerin güvenli bir şekilde saklanması ile hukuka uygun olarak işlenmesinin sağlanması ve kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi amacıyla aşağıdaki teknik ve idari tedbirleri almaktadır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerekğinde veri maskeleyme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri 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.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme kullanılmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- 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.
- Veri kaybı önleme yazılımları kullanılmaktadır.

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

Kişisel verileri imha etmeye (silmeye, yok etmeye ve anonim hale getirmeye) yönelik Üniversite bünyesinde bulunan uygulamalar aşağıdaki gibidir:

Kişisel Verilerin Silinmesi

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.
- Kağıt ortamında bulunan kişisel veriler; karartma yöntemi (çizilerek/boyanarak/silinerek) kullanılarak silinmektedir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünmez hale getirilmesi şeklinde yapılmaktadır.
- Merkezi sunucuda yer alan ofis dosyaları, dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması ile gerçekleştirilmektedir.
- Taşınabilir medyada bulunan kişisel veriler (örneğin flash tabanlı saklama ortamında bulunan veriler) ise şifreli olarak saklanmakta ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.
- Veri tabanlarında bulunan kişisel veriler, ilgili satırların/sütunların ya da tablo içerisinde yer alan hücreler veri tabanı komutları ile (DELETE vb.) silinmektedir.

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

Kişisel Verilerin Yok Edilmesi

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

Kişisel Verilerin Anonim Hale Getirilmesi

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

KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

PERSONEL	BİRİM	GÖREV TANIMI
Arşiv Sorumlusu	Arşiv Sorumlusu	Kişisel verilerin imha edilmesi.

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

Avukat	Hukuk Müşavirliği	İlgili kişilerin taleplerinin alınması, usulüne uygunluğunun kontrolü ve talebin cevaplanması.
Bilgi İşlem Personeli	Bilgi İşlem Daire Başkanlığı Personeli/ Birim Bilgi İşlem Personeli	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması.
İdari İşler Personeli	İdari İşler Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
Personeli	Personel Daire Başkanlığı Personeli/ Birim Personel İşleri Personeli	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

SAKLAMA VE İMHA SÜRELERİNE İLİŞKİN TABLO

- Üniversite bünyesinde bulunan kişisel veriler; ilgili kanunlarda ve mevzuatta öngörülmesi durumunda bu mevzuatta belirtilen süre boyunca saklamaktadır.
- Kişisel verilerin işleme amacı sona ermiş, ilgili mevzuat ve Üniversitenin belirlediği saklama süresinin de sonuna gelmişse, kişisel veriler yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zamanaşımı süreleri esas alınır. Bu durumda kişisel verilere herhangi bir başka amaçla erişim yapılmamaktadır. Kişisel veriler söz konusu süreler sona erdikten sonra imha edilmektedir.

SAKLANAN KİŞİSEL VERİLER		SAKLAMA SÜRESİ	SAKLAMA SÜRESİ	
Kimlik (ad soyad, anne – baba adı, anne kızsık soyadı, doğum tarihi, doğum yeri, medeni hali, nüfus cüzdanı seri sıra no, tc kimlik no gibi)		Öğrenci için 100 yıl, personel için iş ilişkisinin sona	Saklama süresinin bitimini takip eden ilk periyodik	
KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

	ermesinden itibaren 10 yıl	imha işleminde imha edilir.
İletişim (adres no, e-posta adresi, iletişim adres, kayıtlı elektronik posta adresi (KEP), telefonno gibi)	Öğrenci için 100 yıl, personel için iş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Özlük (bordro bilgileri, disiplin soruşturması, işe giriş-çıkış belgesi kayıtları, mal bildirim bilgileri, özgeçmiş bilgileri, performans değerlendirme raporları gibi)	Personelin iş ilişkisi sona erdikten sonra 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Hukuki İşlem (adli makamlarla yazışmalardaki bilgiler, dava dosyasındaki bilgiler gibi)	15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Müşteri İşlem (çağrı merkezi kayıtları)	3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Görsel ve İşitsel Kayıtlar (görsel ve işitsel kayıtlar gibi)	3 ay saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Fiziksel Mekân Güvenliği (çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri, kamera kayıtları gibi)	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Yayınlanma Tarihi

05.04.2021

İşlem Güvenliği (IP adresi bilgileri, internet sitesi giriş çıkış bilgileri, şifre ve parola bilgileri gibi)	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Risk Yönetimi (ticari, teknik, idari risklerin yönetilmesi için işlenen bilgiler gibi)	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Finans (bilanço bilgileri, finansal performans bilgileri, kredi ve risk bilgileri, malvarlığı bilgileri gibi)	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Mesleki Deneyim (diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, transkript bilgileri gibi)	Öğrenci için 100 yıl, personel için iş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
12-Pazarlama (alışveriş geçmişi bilgileri, anket, çerez kayıtları, kampanya çalışmasıyla elde edilen bilgiler)	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Sendika Üyeliği (sendika üyeliği bilgileri gibi)	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Sağlık Bilgileri (engellilik durumuna ait bilgiler, kan grubu bilgisi, kişisel sağlık bilgileri, kullanılan cihaz ve protez bilgileri gibi)	20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.

	KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Yayınlanma Tarihi
		05.04.2021

Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri (ceza mahkûmiyetine ilişkin bilgiler, güvenlik tedbirlerine ilişkin bilgiler gibi)	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Biyometrik Veri (avuç içi bilgileri, parmak izi bilgileri, retina taraması bilgileri, yüz tanıma bilgileri gibi)	Personel iş ilişkisi sürdüğü süre zarfında	İlişği kesildiği anda imha edilir.

PERİYODİK İMHA SÜRELERİ

- Kişisel verilerin imha edilmesine ilişkin yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinir, yok edilir veya anonim hale getirilir. Periyodik imha, tüm kişisel veriler için 6 aylık zaman aralıklarında (Her yılın 1. ve 7. ayının sonunda) gerçekleştirilir.
- Silinen, yok edilen ve anonim hale getirilen verilere ilişkin işlemlerin bulunduğu tutanaklar diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süre ile saklanır.

TUTANAK

- Yukarıda belirtilen silme, yok etme ve anonim hale getirme işlemleri; işlemleri gerçekleştiren ilgili birim müdürü, şefi ve personelinin üçlü imzası ile hazırlanan tutanak ile kayıt altına alınır

KOD	SÜRÜM	DURUM	HAZIRLAYAN	ONAYLAYAN
MÜ-KVKK-PL02	VO	YÜRÜRLÜKTE	Ayşen USLU Bilgi Gv. Yn.	KVKK Kom. Bşk.