l

İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1. Amaç

Bu politikanın amacı, 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat ile düzenleyici kurum kararlarına uygun bir şekilde yürütülen kişisel veri işleme faaliyetleri ve kişisel verilerin korunmasına yönelik benimsenen sistemler konusunda açıklamalarda bulunmak, kurum içinde kişisel veri işlemeyi gerektiren süreçlerin düzenlenmesini ve denetlenmesini sağlamak, kişisel verilerin işlenmesi süreçlerinde yer alan birimlerde kişisel verilerin hukuka uygun şekilde işlenmesi bilincini geliştirmek ve bu bağlamda sorumluluk duygusunu yerleştirmek, çalışan personelin kullandıkları çalışma ortamlarında hassas bilgileri yetkisiz kişilerce erişimini engellemek, kişisel veri işleme süreçlerimiz hakkında öğrencilerimiz, mezunlarımız, çalışan adaylarımız, yetkililerimiz, ziyaretçilerimiz, iş birliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkilileri ile üçüncü kişiler başta olmak üzere, kişisel verileri Üniversitemiz tarafından işlenen kişileri bilgilendirerek veri işleme süreçlerimiz hakkında saydamlığı sağlamaktır.

2. Kapsam

ESOGÜ bünyesinde kullanılan bilgi sistemlerine erişebilen tüm kullanıcıları kapsar.

3. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından ESOGÜ bünyesinde kullanılan bilgi sistemlerine erişebilen tüm kullanıcılar sorumludur.

5. Tanımlar

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, örneğin; karartma, maskeleme, toplulaştırma, veri bozma vb. tekniklerle bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi,

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

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

Katılımcı : Üniversitemiz tarafından düzenlenen herhangi bir etkinlik, kurs veya eğitimlere katılan kişi,

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 : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Örneğin; ad-soyadı, TCKN, cep telefonu numarası, e-posta, iletişim adresi vb.,

Kişisel veri sahibi/ilgilisi : Kişisel verisi işlenen gerçek kişi. Örneğin; çalışanlar, öğrenciler, ziyaretçiler,

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

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

KVK Komisyonu : Üniversitemizin Kişisel Verileri Koruma Kanunu, KVK Kurul kararlarına ve ilgili mevzuat hükümlerine uyum sağlanmasını, düzenlenen politikaların uygulanmasını ve gerekli denetimlerinin gerçekleştirilmesini sağlamakla yükümlü olan Eskişehir Osmangazi Üniversitesi Kişisel Verileri Koruma Komisyonu,

KVK Kurulu/Düzenleyici Kurul : Kişisel Verileri Koruma Kurulu,

KVK Kurumu/Düzenleyici Kurum: Kişisel Verileri Koruma Kurumu,

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

Politika : Eskişehir Osmangazi Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası,

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,

Log Kayıtları: Bilgisayarlarda gerçekleştirilen her etkinliğin kayıt altına alınması,

Rektör : Eskişehir Osmangazi Üniversitesi Rektörü**,**

Talimat : Bir etkinliğin ve/veya işin basamaklarının nasıl yapılacağını anlatan ve prosedürleri destekleyen kısa, basit, anlaşılabilir yazılı dokümanları,

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

Tedarikçi : Üniversitemizin faaliyetlerini yürütürken Üniversitemizin emir ve talimatlarına uygun olarak sözleşme temelli olarak Üniversitemize hizmet sunan taraflar,
Üniversite/ Üniversitemiz : Eskişehir Osmangazi Üniversitesi,
Üniversite yetkilisi : Eskişehir Osmangazi Üniversitesi Rektörü,
Üçüncü kişi : Politika kapsamında farklı bir şekilde tanımlanmamış olan, kişisel verileri politika kapsamında işlenen gerçek kişiler (Örn. Refakatçi, aile bireyleri ve yakınlar),
Veri işleyen : Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi,
Veri sorumlusu : Kişisel verilerin işlenme 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 veya internet sitelerimizi ziyaret eden gerçek kişiler.

4. UYGULAMA

Üniversitemiz KVKK komisyonu tarafından hazırlanan ve onaylanan "Eskişehir Osmangazi Üniversitesi KVK Politikası"nda yer alan "temel ilkeler" başta olmak üzere yürürlükte olan mevzuatta öngörülen tüm hüküm ve koşullar ile hukukun genel ilkelerine uygun olarak gerçekleştirilmektedir.

6. Kurallar

6.1. Kayıt Yönetimi

- Kişisel Veri İşleme Envanterinin Hazırlanması ve belirli periyotlarda güncellenmelidir. Hazırlanan envanter, Veri Sorumluları Sicili Hakkında Yönetmelik'e uygun olmalıdır.
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak ve kurum tarafından hazırlanan kişisel veri işleme envanteri göz önünde bulundurularak kişisel veri saklama ve imha politikası hazırlanmalıdır.
- Kişisel veri barındıran veri tabanının dışarıya aktarımı (dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.) yalnızca yetkilendirilmiş kullanıcılar tarafından yapılmalıdır.

- Özel nitelikli kişisel veriyi barındıran kayıtlar ulusal/uluslararası kabul görmüş güvenli yöntemlerle (şifreli metin olarak, güçlü şifreleme algoritmaları kullanarak, disk seviyesinde şifreleme vb.) saklanmalıdır.
- Kişisel veri barındıran kayıtlar (resimler, ofis dosyaları vb.) güvensiz ortamlarda (yetkisiz erişim sağlanabilen ortak dizin, harici bellek, disk vb.) saklanmamalıdır. Kayıtların saklanmasının zorunlu olduğu durumlarda ulusal/uluslararası standartlar/otoriteler tarafından kabul edilen güvenli yöntemlerden yararlanılmalıdır.
-

6.2. Erişim Kayıtları Yönetimi

- Kişisel verilere gerçekleştirilen erişim kayıtları, kurumun tabi olduğu ilgili mevzuata ve ikincil düzenlemelere uygun şekilde arşivlenmelidir.
- Kişisel veriye gerçekleştirilen erişim kayıtlarının yetkisiz okunması, değiştirilmesi veya silinmesi önlenmelidir.
- Kişisel veriye gerçekleştirilen yetkisiz işlemleri tespit edebilmek için erişim kayıtları analiz edilmelidir.

6.3. Yetkilendirme

- Kullanıcıların sadece erişim yetki matrislerinde yetkilendirildiği kişisel veriye erişmesi sağlanmalıdır. Yetkisiz erişim durumunda veya beklenmeyen bir durum oluştuğunda kişisel veriye erişim varsayılan olarak engellenmelidir. Kişisel veri barındıran tüm ortamlara (web sayfası, dosya vb.) erişim için kimlik doğrulaması yapılmalıdır.
- Kişisel veri barındıran ortamlara (veri tabanı sunucusu, dosya sunucusu vb.) sadece uygulamadan erişim sağlanmalı ve bu ortamlara alternatif ve güvenli olmayan yöntemler (veri tabanı istemcileri

ile doğrudan erişim, güvenli olmayan protokoller ile erişim vb.) ile yapılabilecek yetkisiz erişimler engellenmelidir.

- Kişisel verilerin bulunduğu ortamlar/kaynaklar belirlenmelidir. Belirlenen ortamlar/kaynaklar için erişim denetim politikaları oluşturulmalıdır. Bu politikalarda, kullanıcı rolleri ve erişim yetkilerini açıklayan matris tanımlanmalıdır.

6.4. Şifreleme

- Kişisel verinin paylaşımında sistemler (kurum uygulamaları, dış web servisler) arası iletişim şifreli olarak gerçekleştirilmelidir.
- Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.
- Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için uygun kriptografik yöntemler uygulanmalıdır.

6.5. İlgili Kişi Başvuruları

İlgili kişinin veri sorumlusuna başvuruda bulunabilmesi ve bu başvuruya cevap sürecinin yönetimi için KVK mevzuatı uyarınca talep yönetim süreci talimatı oluşturulmuştur. Ayrıca ilgili kişi başvuru formu üniversitenin web sayfasında da bulunmaktadır.

7. Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

8. İlgili Dokümanlar

PL.17 - UYGULAMA VE VERİ GÜVENLİĞİ POLİTİKASI

PL.17-FR.01 – UYGULAMA SUNUCU ERİŞİMİ YETKİ MATRİSİ FORMU

PL.17-FR.02 - UYGULAMA ERİŞİMİ YETKİLENDİRME FORMU

PL.17-FR.03 - UYGULAMA ERİŞİMİ YETKİ İPTAL FORMU

PL.19 -TL.01- KİŞİSEL VERİLERİN GÜVENLİĞİ TALİMATNAMESİ

Eskişehir Osmangazi Üniversitesi KVK Politikası

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI