

MENTORAVA KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

(Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesine İlişkin)

Son güncelleme: 29.12.2025

Bu Politika; www.mentorava.com internet sitesi ve MentorAva mobil uygulaması üzerinden sunulan hizmetler kapsamında, ALİVA YAZILIM DONANIM VE DANIŞMANLIK ANONİM ŞİRKETİ (“MentorAva” veya “Şirket”) tarafından işlenen kişisel verilerin saklanması, korunması ve işleme amaçlarının ortadan kalkması halinde silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları düzenler.

Politika; Platform ziyaretçileri, kullanıcılar (danışan/katılımcı), sağlık profesyonelleri (bireysel mentörler), kurum hesapları (klinik/egitim kurumu vb.), tedarikçiler ve Şirket çalışanları dâhil olmak üzere Şirket tarafından kişisel verisi işlenen ilgili kişi gruplarını kapsar.

Bu Politika; KVKK aydınlatma metinleri, Gizlilik Politikası ve sözleşme metinleri ile birlikte değerlendirilir. Politika hükümleri ile sözleşme/politika metinleri arasında çelişki olması halinde; ilgili mevzuat hükümleri saklı kalmak kaydıyla, kişisel verilerin korunmasına ilişkin daha yüksek koruma sağlayan hüküm uygulanır.

1. Veri sorumlusu ve iletişim

Veri sorumlusu: ALİVA YAZILIM DONANIM VE DANIŞMANLIK ANONİM ŞİRKETİ

Adres: Sümer Mahallesi 2482/2 Sokak Sky City B Blok No:4/1/26 Merkezefendi / DENİZLİ

MERSİS No: 0053153674800001

Vergi Dairesi/No: Gökpınar / 0531536748

KEP: aliva.yazilim@hs01.kep.tr

KVKK e-posta: kvkk@mentorava.com

Genel iletişim: info@mentorava.com

Çağrı Merkezi: 0 850 885 444 7 (Hafta içi 09.00–18.00)

WhatsApp Destek: 0 532 296 77 92

2. Dayanak

Bu Politika, başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) olmak üzere, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve ilgili sair mevzuat uyarınca hazırlanmıştır.

3. Tanımlar

- Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
- Özel nitelikli kişisel veri: KVKK’da özel koruma öngörülen veri türleri (ör. sağlık verisi).
- Veri işleme: Kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, açıklanması, aktarılması, sınıflandırılması, kullanılmasının engellenmesi dâhil her türlü işlem.

- Silme: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
- Yok etme: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi.
- Anonim hale getirme: Kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
- Periyodik imha: İşleme şartlarının ortadan kalktığı durumlarda, Şirket tarafından belirlenen aralıklarla yapılan silme/yok etme/anonim hale getirme işlemi.

4. Saklamayı ve imhayı gerektiren sebepler

Şirket, kişisel verileri; Platform hizmetlerinin sunulması, sözleşmelerin kurulması/ifası, hukuki yükümlülüklerin yerine getirilmesi, bilgi güvenliği ve suistimalin önlenmesi gibi meşru amaçlarla işler ve saklar.

Kişisel verilerin imhasını gerektiren başlıca haller şunlardır:

- İlgili mevzuatta öngörülen saklama süresinin sona ermesi,
- İşleme amacının ortadan kalkması veya işleme şartlarının sona ermesi,
- İlgili kişinin KVKK kapsamında talepte bulunması ve talebin kabul edilmesi,
- Şirketin re'sen değerlendirmesi sonucunda imha yükümlülüğünün doğması.

5. Saklama ve imhaya ilişkin genel ilkeler

- Hukuka ve dürüstlük kurallarına uygunluk,
- Amaçla bağlantılı, sınırlı ve ölçülü olma (veri minimizasyonu),
- Doğru ve gerektiğinde güncel tutma,
- İşleme amaçları için gerekli süre kadar muhafaza etme,
- Uygun idari ve teknik tedbirlerle güvenliği sağlama,
- İşleme şartları ortadan kalktığında gecikmeksizin imha etme.

6. Kayıt ortamları

Kişisel veriler; Platform'un çalışması için kullanılan uygulama veritabanları ve sunucular, yedekleme sistemleri, e-posta sistemleri, destek/talep yönetim sistemleri, log kayıtları, muhasebe/finans sistemleri ve yetkilendirilmiş personelin erişebildiği iş uygulamalarında saklanabilir.

Şirket; altyapı, barındırma ve/veya destek hizmetleri kapsamında tedarikçi sistemlerinden yararlanabilir. Bu durumda; tedarikçilerle KVKK'ya uygun sözleşmesel ve teknik/idari tedbirler tesis edilir ve yalnızca hizmetin gerektirdiği ölçüde işlem yapılır.

7. İdari ve teknik tedbirler

Şirket; kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla makul ve uygun idari ve teknik tedbirleri uygular. Bu tedbirler; yetki matrisi ve rol bazlı erişim, kayıt altına alma (log), şifreleme/maskeleme, yedekleme, sızma ve güvenlik kontrolleri, tedarikçi denetimi, gizlilik taahhütleri ve eğitimler gibi önlemleri içerebilir.

8. Silme, yok etme ve anonim hale getirme yöntemleri

Şirket, imha işlemlerini verinin bulunduğu ortamın niteliğine göre uygun yöntemlerle gerçekleştirir. Başlıca yöntemler aşağıdaki gibidir:

8.1. Silme yöntemleri

- Veritabanı kayıtlarının kalıcı olarak silinmesi (hard delete) veya geri döndürülemeyecek şekilde kaldırılması,
- Mantıksal silme/erişim kısıtlama (soft delete) ve ilk periyodik imha döneminde fiziksel silme,
- Uygulama düzeyinde erişim yetkilerinin kaldırılması ve anahtar/jeton iptali,
- Yedeklerden geri getirildiğinde de silmeyi sağlayacak şekilde silme planları (yedeklerden tenzil).

8.2. Yok etme yöntemleri

- Fiziksel ortamların (kağıt, taşınabilir bellek vb.) parçalanması, yakılması veya güvenli imha hizmetiyle yok edilmesi,
- Dijital ortamların geri getirilemeyecek şekilde üzerine yazma (secure wipe) veya kriptografik imha (anahtarın yok edilmesi).

8.3. Anonim hale getirme yöntemleri

- Maskeleme veya takma adlandırma (pseudonymization) ve kimlik bağıını koparma,
- Veri kümesini toplulaştırma (aggregation) ve istatistiksel olarak kimliği belirlenebilirliği ortadan kaldırma,
- Hash'leme ve geri döndürülemeyecek biçimde ayırt edici değerleri kaldırma,
- Kayıtların veri setinden çıkarılması veya alan bazında genelleştirme (ör. yaş aralığı).

9. Saklama süreleri

Aşağıdaki süreler; Platform'un işleyişi, sözleşmesel ilişkilerin ispatı, vergisel yükümlülükler, bilgi güvenliği ve ilgili mevzuat çerçevesinde belirlenmiştir. Bir uyuşmazlığın, denetimin veya resmi incelemenin varlığı halinde; ilgili veriler, süreç sonuçlanıncaya kadar ayrıca saklanabilir.

Not: Ödeme aracı (kart) bilgileri Şirket sistemlerinde saklanmaz. Ödeme kuruluşlarının saklama ve güvenlik yükümlülükleri kendi mevzuatları çerçevesindedir.

Veri kategorisi / örnek	Amaç	Saklama süresi (genel)	İmha yöntemi (örnek)
-------------------------	------	------------------------	----------------------

Sözleşmeler ve ticari kayıtlar (üyelik, iş ortaklığı, mesafeli satış, ön bilgilendirme, iptal/ iade kayıtları)	Sözleşmenin ifası, ispat, uyumsuzluk yönetimi	İlişkinin sona ermesinden itibaren 10 yıl	Kalıcı silme; yedeklerden tenzil
Muhasebe ve faturalama kayıtları (e-Fatura/e-Arşiv/e-SMM, mutabakat, komisyon, ödeme/ aktarım kayıtları)	Vergisel yükümlülükler ve denetim	10 yıl	Kalıcı silme
Hesap ve iletişim bilgileri (ad-soyad/unvan, e-posta, telefon, rol, profil bilgileri)	Hesap işletimi, destek, güvenlik	Hesap kapanışı + 3 yıl	Mantıksal silme; süre sonunda kalıcı silme/ anonimleştirme
Satıcı/kurum doğrulama belgeleri (vergi levhası, yetki belgesi, mesleki belge/diploma vb.)	Uygunluk değerlendirmesi ve ispat	İlişki süresince + 10 yıl	Mantıksal silme → süre sonunda kalıcı silme
Kurs/webinar erişim ve katılım kayıtları (erişim logları, satın alma ve görüntüleme kayıtları)	Hizmetin ifası, suistimal önleme, ispat	Hizmet bitimi + 3 yıl	Mantıksal silme; süre sonunda kalıcı silme
Destek/şikayet kayıtları (ticket, e-posta yazışmaları)	Müşteri ilişkileri ve ispat	3 yıl	Kalıcı silme
Güvenlik ve erişim logları (oturum, hata, güvenlik kayıtları)	Bilgi güvenliği ve suistimal önleme	2 yıl	Maskeme; süre sonunda kalıcı silme
Çerez tercih ve izin kayıtları	Tercih yönetimi ve ispat	İzin geri çekilene kadar + 1 yıl	Kalıcı silme
Ticari ileti izinleri ve tercihleri	Ticari ileti gönderimi ve ispat	İzin geri çekilene kadar + 1 yıl	Kalıcı silme

Fiziki güvenlik kayıtları (kamera kaydı) – varsa	Fiziki güvenlik	30 gün (olay/ inceleme varsa süreç sonuna kadar)	Üzerine yazma veya kalıcı silme
--	-----------------	--	---------------------------------

10. Periyodik imha süresi

Şirket, periyodik imha süresini 6 (altı) ay olarak belirlemiştir. İşleme şartlarının ortadan kalktığı tespit edilen kişisel veriler; en geç ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.

Şirket, gerekli görmesi halinde periyodik imha işlemlerini daha kısa aralıklarla gerçekleştirebilir.

11. İlgili kişi başvuruları

İlgili kişiler, KVKK'nın 11. maddesi kapsamındaki haklarını kullanmak için "İlgili Kişi Başvuru Formu" üzerinden Şirket'e başvurabilir. Başvurular, kimlik doğrulama ve yetki kontrolü sonrasında değerlendirilir ve mevzuatta öngörülen süreler içinde yanıtlanır.

12. Yürürlük ve güncelleme

Bu Politika, Platform'da yayımlandığı tarihte yürürlüğe girer. Şirket, mevzuat ve operasyonel ihtiyaçlar doğrultusunda Politikayı güncelleyebilir. Güncel versiyon Platform üzerinden erişime açık tutulur.