TARİH	18.05.2026
KURUM	MENTEŞE BELEDİYE BAŞKANLIĞI
DETSİS NUMARASI	61943286
VERGİ KİMLİK NUMARASI	6150383376
İLETİŞİM E POSTA ADRESİ	kvkk@mentese.bel.tr
KEP ADRESİ	mentesebel@hs01.kep.tr
KURUM WEB SİTESİ	www.mentese.bel.tr
ADRES	Şeyh Mah. Belediye Sk. No:11 Menteşe/MUĞLA

VERİ İHLALİ MÜDAHALE POLİTİKASI

1. AMAÇ

Bu politikanın amacı, Menteşe Belediye Başkanlığı tarafından işlenen kişisel verilerin hukuka aykırı olarak işlenmesi, yetkisiz kişilerce erişilmesi, ifşa edilmesi, kaybolması, değiştirilmesi, silinmesi, yok edilmesi veya güvenliğinin ihlal edilmesi hallerinde uygulanacak tespit, müdahale, bildirim, kayıt altına alma, iyileştirme ve raporlama süreçlerini belirlemektir.

2. KAPSAM

Bu politika; Menteşe Belediye Başkanlığı birimleri, çalışanları, geçici/sözleşmeli personeli, hizmet alımı yoluyla görev yapan personel, tedarikçiler, veri işleyenler ve belediye adına kişisel veri işleme süreçlerine dahil olan tüm kişi ve birimleri kapsar. Politika, elektronik ve fiziki ortamlardaki tüm kişisel veri ihlali şüpheleri ile doğrulanmış kişisel veri ihlallerine uygulanır.

3. DAYANAK

Bu politika; 6698 sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verileri Koruma Kurulu kararları, Kişisel Veri Güvenliği Rehberi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve ilgili diğer resmi mevzuat esas alınarak hazırlanmıştır.

4. TANIMLAR VE KISALTMALAR

KAVRAM	AÇIKLAMA
Kurum	Menteşe Belediye Başkanlığı.
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu.
Kurul	Kişisel Verileri Koruma Kurulu.
Kurum (KVKK)	Kişisel Verileri Koruma Kurumu.
Kişisel Veri İhlali	Kişisel verilerin hukuka aykırı olarak işlenmesi, erişilmesi, açıklanması, aktarılması, kaybolması, değiştirilmesi, silinmesi veya veri güvenliğini etkileyen benzeri olaylar.
İhlal Şüphesi	Kişisel veri güvenliğini etkileyebileceği değerlendirilen ancak henüz doğrulanmamış olay veya bulgu.
KVK Komisyonu	Kişisel verilerin korunması süreçlerinin idari takibini yapmak üzere kurum içinde görevlendirilen komisyon veya sorumlu ekip.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.

5. VERİ İHLALİ ÖRNEKLERİ

- Kişisel veri içeren evrakın kaybolması, yanlış kişiye gönderilmesi veya yetkisiz kişilerce görülmesi.
- Kişisel veri içeren e-posta, KEP, faks veya fiziki gönderinin yanlış alıcıya iletilmesi.
- Bilgi sistemlerine yetkisiz erişim, zararlı yazılım bulaşması, fidye yazılımı, hesap ele geçirilmesi veya yetkisiz veri indirilmesi.
- Kişisel veri içeren taşınabilir bellek, bilgisayar, telefon, tablet veya dosyanın kaybolması ya da çalınması.
- Kişisel verilerin yetki sınırını aşan personel veya üçüncü kişiler tarafından görüntülenmesi, kopyalanması, paylaşılması veya ifşa edilmesi.
- Özel nitelikli kişisel verilerin yetkisiz ortamda saklanması, şifresiz aktarılması veya yetkisiz kişilere açıklanması.

6. GÖREV VE SORUMLULUKLAR

- Tüm çalışanlar ve veri işleme süreçlerine dahil olan kişiler, ihlal şüphesi doğuran her olayı gecikmeksizin birim amirine ve KVK Komisyonuna bildirmekle yükümlüdür.
- Birim amirleri, ihlal şüphesinin ilk tespitini yapmak, delillerin korunmasını sağlamak ve KVK Komisyonuna gerekli bilgi ve belgeleri iletmekle sorumludur.
- Bilgi işlem veya teknik sorumlu birim, elektronik sistemlerdeki ihlal şüphelerinde olayın teknik analizini yapmak, logları korumak, etkilenen sistemleri izole etmek ve gerekli teknik tedbirleri almakla sorumludur.
- KVK Komisyonu, ihlal değerlendirmesini yapmak, Kurula ve ilgili kişilere bildirim gerekip gerekmediğini belirlemek, bildirim metinlerini hazırlamak, kayıtları tutmak ve düzeltici/önleyici faaliyetleri takip etmekle sorumludur.
- Hukuk/insan kaynakları/disiplin birimleri, ihlalin niteliğine göre idari, disipliner veya hukuki süreçlerin yürütülmesinden sorumludur.

7. İHLAL ŞÜPHESİNİN BİLDİRİLMESİ

İhlal şüphesi öğrenildiğinde gecikmeksizin KVK Komisyonuna bildirilir. Bildirimde mümkün olduğu ölçüde olayın tarihi, öğrenilme tarihi, ihlal şüphesinin niteliği, etkilenen sistem veya evrak, veri kategorileri, ilgili kişi grupları, tahmini kişi/kayıt sayısı, alınan ilk tedbirler ve bildirimi yapan kişinin iletişim bilgileri yer alır.

İhlal şüphesi sözlü olarak öğrenilmişse olay, gecikmeksizin yazılı kayıt altına alınır. Elektronik olaylarda log kayıtları, ekran görüntüleri ve sistem kayıtları korunur; fiziki olaylarda tutanak düzenlenir.

8. ÖN DEĞERLENDİRME VE RİSK ANALİZİ

- Olayın kişisel veri ihlali oluşturup oluşturmadığı değerlendirilir.
- Etkilenen kişisel veri kategorileri, özel nitelikli veri bulunup bulunmadığı, veri miktarı ve ilgili kişi grupları belirlenir.
- İhlalin gizlilik, bütünlük ve erişilebilirlik üzerindeki etkisi incelenir.
- İlgili kişiler bakımından doğabilecek zarar, ayrımcılık, kimlik hırsızlığı, finansal kayıp, itibar kaybı, özel hayatın ihlali veya hak kaybı riski değerlendirilir.
- İhlalin devam edip etmediği ve yayılma riski belirlenir.

9. MÜDAHALE VE KONTROL ALTINA ALMA

- Etkilenen sistem, hesap veya cihazlar gerekli ise geçici olarak izole edilir.
- Yetkisiz erişim şüphesi bulunan hesapların parolaları değiştirilir, oturumlar sonlandırılır ve erişim yetkileri gözden geçirilir.
- Yanlış alıcıya gönderilen kişisel veri içeren evrak veya e-postanın silinmesi/iadesi talep edilir; mümkünse teyit alınır.
- Zararlı yazılım, siber saldırı veya sistem açığı halinde gerekli teknik müdahale yapılır ve ilgili kayıtlar korunur.
- Özel nitelikli kişisel veri etkilenmişse şifreleme, erişim kısıtlama, fiziksel güvenlik ve güvenli aktarım tedbirleri derhal gözden geçirilir.

10. KURULA VE İLGİLİ KİŞİLERE BİLDİRİM

Kişisel veri ihlalinin gerçekleştiğinin tespit edilmesi halinde, ihlalden etkilenen kişisel verilerin niteliği, ilgili kişi sayısı, ihlalin muhtemel sonuçları ve risk düzeyi dikkate alınarak Kurula bildirim gerekip gerekmediği KVK Komisyonu tarafından değerlendirilir.

Kurula bildirim yapılması gereken hallerde bildirim, ihlalin öğrenilmesinden itibaren en kısa sürede ve kural olarak 72 saat içinde yapılır. Bildirimin 72 saat içinde yapılamaması halinde gecikmenin nedeni ayrıca açıklanır.

İlgili kişilerin ihlalden etkilenme ihtimali bulunduğu hallerde, ilgili kişiler mümkün olan en kısa sürede ve açık, sade, anlaşılır bir dille bilgilendirilir. İlgili kişi bildiriminde ihlalin ne olduğu,

etkilenen veri kategorileri, muhtemel sonuçlar, alınan tedbirler, ilgili kişilerin alabileceği önlemler ve iletişim kanalı belirtilir.

11. İHLAL KAYDI VE DOKÜMANTASYON

Tüm ihlal şüpheleri ve doğrulanmış ihlaller, sonuç ne olursa olsun kayıt altına alınır. Kayıtta olayın tarihi, öğrenilme tarihi, bildirim yapan kişi, ihlal türü, etkilenen veri kategorileri, ilgili kişi grupları, alınan tedbirler, bildirim kararları, Kurula/ilgili kişilere yapılan bildirimler ve düzeltici faaliyetler yer alır.

İhlal kayıtları, yetkili kişiler dışında erişime kapalı tutulur ve Kişisel Veri Saklama ve İmha Politikası ile ilgili mevzuat çerçevesinde saklanır.

12. DÜZELTİCİ VE ÖNLEYİCİ FAALİYETLER

- İhlalin kök nedeni analiz edilir ve tekrarını önlemek için teknik/idari tedbir planı hazırlanır.
- Erişim yetkileri, parola politikaları, loglama, yedekleme, şifreleme ve güvenli aktarım süreçleri gözden geçirilir.
- Personel eğitimleri, gizlilik taahhütleri ve kurumsal prosedürler ihtiyaç halinde güncellenir.
- Veri işleyen veya tedarikçi kaynaklı ihlallerde sözleşmesel yükümlülükler, denetim kayıtları ve veri güvenliği taahhütleri gözden geçirilir.

13. DİSİPLİN VE HUKUKİ SÜREÇ

İhlalin personel kusuru, ihmal, yetki aşımı veya kasıtlı davranıştan kaynaklandığının tespiti halinde Kişisel Veri İhlali Disiplin Politikası ve ilgili personel mevzuatı kapsamında işlem yapılır. Suç şüphesi bulunan hallerde yetkili mercilere başvuru hakkı saklıdır.

14. İLGİLİ DOKÜMANLAR

- Kişisel Veri İhlali Disiplin Politikası
- Kişisel Veri Saklama ve İmha Politikası
- Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Politikası
- Genel Güvenlik Talimatı
- Kötü Niyetli Yazılımlara Karşı Korunma Prosedürü
- Kullanıcı Parola Yönetimi Prosedürü

REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
V01		18.05.2026