TARİH	12.07.2026
DOKÜMAN KODU	PPT-09
VERSİYON	V04
KURUM	FİLYOS BELEDİYE BAŞKANLIĞI
DETSİS NUMARASI	66666329
VERGİ KİMLİK NUMARASI	1620053082
İLETİŞİM E-POSTA / TELEFON	kvkk@filyos.bel.tr / info@filyos.bel.tr / +90 372 623 10 18
KEP ADRESİ	filyosbldbsk@hs01.kep.tr
KURUM WEB SİTESİ / ADRES	www.filyos.bel.tr / Hisarönü Mahallesi Gazi Hakan Mızrak Caddesi No:19 Filyos/Çaycuma/ZONGULDAK
DOKÜMAN TÜRÜ	POLİTİKA / PROSEDÜR / TALİMAT

VERİ İHLALİ MÜDAHALE POLİTİKASI

1. AMAÇ

Bu politikanın amacı, Filyos 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 ve iyileştirme süreçlerini belirlemektir.

2. KAPSAM

Bu doküman; FİLYOS BELEDİYE BAŞKANLIĞI birimleri, çalışanları, geçici/sözleşmeli personeli, hizmet alımı yoluyla görev yapan personel, meclis ve encümen süreçleri, tedarikçiler, veri işleyenler, belediye adına kişisel veri işleme süreçlerine dahil olan tüm kişi ve birimler ile elektronik/fiziki kayıt ortamlarını kapsar.

3. DAYANAK

Bu doküman; 6698 sayılı Kişisel Verilerin Korunması Kanunu, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Veri Sorumluları Sicili Hakkında Yönetmelik, Kişisel Verileri Koruma Kurulu kararları, Kişisel Veri Güvenliği Rehberi, 5393 sayılı Belediye Kanunu ve Filyos Belediyesi hizmet süreçleri esas alınarak hazırlanmıştır.

4. TANIMLAR VE KISALTMALAR

KAVRAM	AÇIKLAMA
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu.
Kurul	Kişisel Verileri Koruma Kurulu.

Kurum	Kişisel Verileri Koruma Kurumu.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Özel Nitelikli Kişisel Veri	KVKK m.6 kapsamında sayılan sağlık, ceza mahkûmiyeti, biyometrik/genetik veri ve diğer özel nitelikli kişisel veriler.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaç ve vasıtalarını belirleyen gerçek veya tüzel kişi.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi.
İlgili Kullanıcı	Kişisel verilere görev ve yetkisi kapsamında erişen kişi veya birim.
Kayıt Ortamı	Kişisel verilerin bulunduğu elektronik veya fiziki ortam.

5. GÖREV VE SORUMLULUKLAR

- Belediye Başkanı ve üst yönetim, kişisel veri güvenliği kültürünün oluşturulması, kaynak tahsisi, onay ve gözetim faaliyetlerinden sorumludur.
- KVK Komisyonu veya görevlendirilen sorumlu ekip, dokümanların güncelliğini, aydınlatma süreçlerini, ilgili kişi başvurularını, ihlal yönetimini, envanter ve VERBİS uyumunu takip eder.
- Birim amirleri, kendi birim süreçlerinde kişisel verilerin amaçla bağlantılı, sınırlı ve ölçülü işlenmesini, erişim yetkilerinin kontrolünü ve personel farkındalığını sağlar.
- Bilgi işlem/teknik sorumlular, ağ, sistem, kullanıcı hesabı, yedekleme, loglama, parola, zararlı yazılım ve yetki kontrollerinin uygulanmasını sağlar.
- Tüm çalışanlar, gizlilik, veri minimizasyonu, güvenli aktarım, temiz masa/temiz ekran ve ihlal bildirimi kurallarına uymakla yükümlüdür.
- Tedarikçiler ve veri işleyenler, sözleşme, protokol ve taahhütlerde yer alan veri güvenliği yükümlülüklerine uygun hareket eder.

6. 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, kamera kayıt cihazı veya dosyanın kaybolması ya da çalınması.
- Özel nitelikli kişisel verilerin yetkisiz ortamda saklanması, şifresiz aktarılması veya yetkisiz kişilere açıklanması.

7. İHLAL ŞÜPHESİNİN BİLDİRİLMESİ

- İhlal şüphesi öğrenildiğinde gecikmeksizin birim amiri ve KVK Komisyonuna bildirilir. Bildirimde olay tarihi, öğrenilme tarihi, ihlal türü, etkilenen sistem/evrak, veri kategorileri, ilgili kişi grupları, tahmini kişi/kayıt sayısı, alınan ilk tedbirler ve bildirimi yapan kişinin bilgileri yer alır.

• 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, etkilenen veri kategorileri, özel nitelikli veri bulunup bulunmadığı, veri miktarı, ilgili kişi grupları ve ihlalin gizlilik/bütünlük/erişilebilirlik etkisi değerlendirilir.

• Kimlik hırsızlığı, ayrımcılık, finansal kayıp, özel hayatın ihlali, itibar kaybı, hak kaybı, sosyal yardım/sağlık bilgisi ifşası ve hukuki riskler dikkate alınır.

9. MÜDAHALE VE KONTROL ALTINA ALMA

• Etkilenen sistem, hesap veya cihazlar gerekli ise izole edilir; parolalar değiştirilir, oturumlar sonlandırılır ve erişim yetkileri gözden geçirilir.

• Yanlış alıcıya gönderilen bilgi için silme/iade talep edilir; mümkünse teyit alınır. Zararlı yazılım veya sistem açığı halinde teknik müdahale yapılır ve deliller korunur.

• Özel nitelikli 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 Kurula bildirim gerekip gerekmediği KVK Komisyonu tarafından değerlendirilir. Bildirim yapılması gereken hallerde ihlalin öğrenilmesinden itibaren en kısa sürede ve kural olarak 72 saat içinde bildirim yapılır; gecikme varsa nedeni açıklanır.

• İlgili kişilerin ihlalden etkilenme ihtimali varsa, ihlalin ne olduğu, etkilenen veri kategorileri, muhtemel sonuçlar, alınan tedbirler, kişilerin alabileceği önlemler ve iletişim kanalı açık, sade ve anlaşılır dille bildirilir.

11. KAYIT, KÖK NEDEN VE DÜZELTİCİ FAALİYET

• Tüm ihlal şüpheleri ve doğrulanmış ihlaller kayıt altına alınır. Kayıtta olayın tarihi, öğrenilme tarihi, bildirim yapan kişi, ihlal türü, etkilenen veri kategorileri, ilgili kişi grupları, alınan tedbirler, bildirim kararları ve düzeltici faaliyetler yer alır.

• İhlalin kök nedeni analiz edilir; erişim yetkileri, parola politikaları, loglama, yedekleme, şifreleme, güvenli aktarım, tedarikçi sözleşmeleri ve personel eğitimleri güncellenir.

TEKNİK VE İDARİ TEDBİRLER

Teknik Tedbirler

• Ağ güvenliği ve uygulama güvenliği tedbirleri uygulanır; güvenlik duvarı, güncel antivirüs/EDR, yama yönetimi ve güvenli yapılandırma kontrolleri takip edilir.

• Kullanıcı hesapları kişiye özel açılır; ortak hesap kullanımı zorunlu haller dışında yasaktır ve istisnalar kayıt altına alınır.

• Erişim logları, 5651 ve ilgili bilgi güvenliği gereklilikleri kapsamında kullanıcı müdahalesi olmayacak şekilde tutulur, korunur ve yalnızca yetkili kişilerce incelenir.

• Yetki matrisi oluşturulur; görev değişikliği, işten ayrılış, sözleşme bitişi veya hizmet sonlanması halinde erişimler gecikmeksizin kapatılır.

• Özel nitelikli kişisel veriler elektronik ortamda şifreli, erişimi kısıtlı ve ayrı yetkilendirme ile tutulur; e-posta ile aktarım zorunluysa şifreli gönderim ve ayrı kanal parola iletimi uygulanır.

• Yedekleme, geri dönüş testi, fiziksel ortam güvenliği, taşınabilir medya kontrolü, güvenli silme ve arşiv güvenliği süreçleri uygulanır.

İdari Tedbirler

- Kişisel veri işleme envanteri ve saklama-imha matrisi birim süreçleriyle eşleştirilir; yeni hizmet veya sistem devreye alınmadan önce veri koruma değerlendirmesi yapılır.
- Aydınlatma metinleri ilgili başvuru formlarında, hizmet noktalarında, web sitesinde ve gerektiğinde fiziksel alanlarda erişilebilir kılınır.
- Çalışanlara ve ilgili görev gruplarına periyodik KVKK, bilgi güvenliği, ihlal bildirimi, parola ve güvenli aktarım eğitimleri verilir.
- Tedarikçi ve veri işleyen sözleşmeleri, kişisel veri güvenliği, gizlilik, alt işleyen, ihlal bildirimi, denetim ve iade/imha hükümleri içerecek şekilde düzenlenir.
- Kişisel veriler kâğıt ortamında kilitli dolap/arşivde; elektronik ortamda yetki sınırlaması ile saklanır. Fazla, güncel olmayan veya amaç dışı veri işlenmemesi esastır.
- İhlal şüphesi halinde deliller korunur, olay kayıt altına alınır ve KVK Komisyonuna derhal bildirilir.

İLGİLİ DOKÜMANLAR

- Kişisel Veri İşleme Envanteri
- Kişisel Veri Saklama ve İmha Politikası
- İlgili Kişi Başvuru Formu
- Veri İhlali İlk Bildirim Formu
- Genel Güvenlik Talimatı
- Kullanıcı Parola Yönetimi Prosedürü
- Tedarikçi ve Veri İşleyen Yönetimi Prosedürü
- Kamera Kayıt Sistemi Yönetimi Prosedürü

REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
V04	Kapsamlı revizyon.	12.07.2026