TARİH	12.07.2026
DOKÜMAN KODU	PPT-12
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

BİLGİ GÜVENLİĞİ VE ERİŞİM YETKİLENDİRME POLİTİKASI

1. AMAÇ

Bu dokümanın amacı, Filyos Belediye Başkanlığı bünyesinde kişisel verilerin korunması, bilgi güvenliği, erişim yetkilendirme, fiziksel güvenlik, tedarikçi yönetimi, çerez yönetimi, ihlal müdahalesi ve saklama-imha süreçlerinin hukuka uygun, ölçülebilir, denetlenebilir ve kurumsal şekilde yürütülmesini sağlamaktır.

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. UYGULAMA ESASLARI

- Kişisel veri işleme faaliyetleri envanterde tanımlanan amaç, hukuki sebep, veri kategorisi, alıcı grubu, saklama süresi ve güvenlik tedbirleriyle uyumlu yürütülür.
- Yeni hizmet, web formu, başvuru kanalı, tedarikçi, yazılım veya kamera alanı devreye alınmadan önce ilgili aydınlatma metni, açık rıza ihtiyacı, veri minimizasyonu, saklama süresi ve aktarım riski değerlendirilir.
- Filyos Belediyesi web sitesi, Dilek & Şikâyet Formu, Başkana Mesaj, nikâh işlemleri, halı saha/düğün salonu tahsisi, ruhsat/imar, sosyal yardım, zabıta, ihale, meclis/encümen ve duyuru süreçleri ayrı işleme faaliyeti olarak ele alınır.
- Özel nitelikli kişisel veriler, yalnızca kanuni zorunluluk veya açık ve ölçülü bir süreç gerekliliği bulunması halinde işlenir; erişim yetkisi daraltılır ve güvenli aktarım uygulanır.
- Yurt dışına aktarım ihtimali bulunan çerez, sosyal medya, bulut, SMS/e-posta ve web analitik hizmetleri için KVKK m.9 kapsamında değerlendirme yapılır; hukuki mekanizma olmadan düzenli aktarım yapılmaz.

7. KAYIT, KANIT VE RAPORLAMA

- Bu doküman kapsamında yapılan işlemler; başvuru kayıtları, tutanaklar, erişim/yetki kayıtları, eğitim listeleri, ihlal formları, imha tutanakları, tedarikçi sözleşmeleri ve denetim raporlarıyla kanıtlanır.
- Kayıtlar saklama-imha politikasında belirtilen süreler boyunca yetkisiz erişime kapalı şekilde muhafaza edilir.

8. GÖZDEN GEÇİRME VE SÜREKLİ İYİLEŞTİRME

- Doküman yılda en az bir kez veya mevzuat, sistem, hizmet, organizasyon, web sitesi, kamera alanı, tedarikçi veya veri işleme faaliyeti değiştiğinde gözden geçirilir.
- Denetimlerde tespit edilen uygunsuzluklar için düzeltici/önleyici faaliyet planı hazırlanır ve tamamlanma durumu takip edilir.

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