TARİH	12.07.2026
DOKÜMAN KODU	PPT-06
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

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Bu politikanın amacı, Filyos Belediye Başkanlığı tarafından işlenen kişisel verilerin hangi kayıt ortamlarında, hangi hukuki sebeplerle ve ne kadar süreyle saklanacağını; işleme şartları ortadan kalktığında silme, yok etme veya anonim hale getirme yöntemlerini ve periyodik imha sürecini 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. İLGİLİ KİŞİ GRUPLARI VE VERİ KATEGORİLERİ

- Vatandaşlar, başvuru sahipleri, çalışanlar, aday çalışanlar, stajyerler, eski çalışanlar, meclis/encümen üyeleri, muhtarlar, tedarikçi/alt işveren çalışanları, ziyaretçiler, halı saha/düğün salonu kullanıcıları, sosyal yardım başvuru sahipleri, ruhsat/imar/ihale süreç tarafları ve diğer üçüncü kişiler.
- Kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri/vatandaş işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, görsel/işitsel kayıtlar, sağlık bilgileri, ceza mahkûmiyeti ve güvenlik tedbirleri ilweb sitesi hizmetlerine özgü tapu/ada/parsel, ruhsat, sosyal yardım ve başvuru bilgileri.

7. SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

- 5393 sayılı Belediye Kanunu, 2464 sayılı Belediye Gelirleri Kanunu, 3194 sayılı İmar Kanunu, 4734 sayılı Kamu İhale Kanunu, 4735 sayılı Kamu İhale Sözleşmeleri Kanunu, 2886 sayılı Devlet İhale Kanunu, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, 657 sayılı Devlet Memurları Kanunu, 4857 sayılı İş Kanunu, 5510 sayılı Kanun, 6331 sayılı Kanun, 213 sayılı Vergi Usul Kanunu, 6183 sayılı Kanun, 3071 sayılı Kanun, 4982 sayılı Kanun, 7201 sayılı Tebligat Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu, 3572 sayılı Kanun, 5326 sayılı Kabahatler Kanunu, 5651 sayılı Kanun, 1593 sayılı

Umumi Hıfzıssıhha Kanunu, 5199 sayılı Hayvanları Koruma Kanunu ve sair ilgili mevzuat saklama dayanakları arasındadır.

- Saklama süresi açıkça düzenlenmemişse, hizmetin gerektirdiği süre, denetim/teftiş süreleri, zamanaşımı süreleri, hukuki uyuşmazlık ihtimali, arşiv yükümlülüğü ve veri minimizasyonu ilkesi birlikte değerlendirilir.

8. KAYIT ORTAMLARI

- Kâğıt dosya ve arşivler, dilekçe ve başvuru evrakları, EBYS ve EBYS kayıtları, web sitesi/veri tabanı, e-posta/KEP, muhasebe ve tahakkuk sistemleri, kamera kayıt cihazları, log sunucuları, yedekleme ortamları, taşınabilir medya, yazıcı/fotokopi bellekleri vweb sitesi birimlerinde kullanılan uygulamalar kayıt ortamlarıdır.
- Kayıt ortamı değiştiğinde envanter, saklama süresi ve imha yöntemi güncellenir.

9. SAKLAMA SÜRESİ BELİRLEME ESASLARI

- Her süreç için saklama süresi; envanterdeki işleme amacı, veri kategorisi, hukuki sebep, alıcı grubu, kayıt ortamı ve mevzuat dayanağı ile birlikte belirlenir.
- Kamera kayıtları yalnızca güvenlik amacıyla gerekli süre kadar saklanır; olay/denetim/hukuki süreç varsa ilgili kayıt ayrı delil dosyasına alınır.
- Çerez ve web logları teknik güvenlik ve mevzuat gerekliliklerıyle sınırlı tutulur; zorunlu olmayan çerezlerde tercih/açık rıza kayıtları ayrıca saklanır.
- Özel nitelikli kişisel veriler, kanuni zorunluluk veya ilgili süreç gerekliliği sona erdiğinde erişimi kısıtlanarak imha listesine alınır.
- Hukuki uyuşmazlık, denetim, soruşturma veya resmi talep halinde imha işlemi ilgili dosya bakımından askıya alınabilir.

10. İMHA YÖNTEMLERİ

- Kâğıt ortamındaki kişisel veriler çapraz kesim/kâğıt imha makinesi, güvenli imha hizmeti veya tutanaklı yakma/parçalama yöntemiyle yok edilir.
- Elektronik dosyalar güvenli silme, erişilemez kılma, kriptografik yok etme, veri tabanı kayıtlarının kontrollü silinmesi veya ortamın fiziksel imhası yöntemleriyle imha edilir.
- Taşınabilir medya, disk ve cihazlar güvenli silme/de-manyetize/fiziksel imha süreçlerinden geçirilir. İmha işlemi tutanakla kayıt altına alınır.
- Anonim hale getirme için maskeleme, toplulaştırma, örnekleme, genelleştirme, kayıt/değişken çıkarma, gürültü ekleme, k-anonimlik, l-çeşitlilik ve t-yakınlık gibi yöntemler kullanılabilir.

11. PERİYODİK İMHA VE TUTANAK

- Periyodik imha kontrolleri en geç altı ayda bir yapılır. İmha listesinde veri kategorisi, süreç, kayıt ortamı, saklama süresi, imha tarihi, yöntem, sorumlu birim ve tutanak bilgisi yer alır.
- İmha tutanakları yetkili kişiler dışında erişime kapalı tutulur ve politika/envanterde belirlenen süre boyunca saklanır.

12. AYDINLATMA, BAŞVURU VE HAK KULLANIM KAYITLARI

- Aydınlatma metinleri, başvuru formları, açık rıza metinleri, ilgili kişi başvuru formları, başvuru değerlendirme yazıları ve cevap kayıtları, ispat yükümlülüğü ve hukuki uyuşmazlık ihtimali dikkate alınarak saklanır.
- İlgili kişi başvurularında kimlik teyidi için alınan belgeler, yalnızca başvurunun değerlendirilmesi, cevaplanması ve olası hukuki süreçlerin yönetimi amacıyla işlenir; başvuru sonuçlandığında gereksiz kopyalar imha edilir.

• Açık rıza kayıtları, rızanın alındığı tarih, yöntem, kapsam, metin versiyonu ve geri alma talebiyle birlikte kayıt altına alınır. Rıza geri çekildiğinde, rızaya dayalı işleme faaliyeti durdurulur; saklama gerektiren hukuki sebep yoksa ilgili veri imha sürecine alınır.

13. AKTARIM VE YURT DIŞI AKTARIM KAYITLARI

• Kişisel verilerin yetkili kamu kurumlarına, bankalara, KEP/e-posta/SMS hizmet sağlayıcılarına, bilişim tedarikçilerine, arşiv ve danışmanlık hizmet sağlayıcılarına aktarılması; süreç, amaç, hukuki sebep ve alıcı grubu bazında envanterde gösterilir.

• Web sitesi, çerez, sosyal medya, SMS/e-posta veya bulut altyapısı nedeniyle yurt dışına aktarım ihtimali varsa KVKK m.9 kapsamında uygun mekanizma değerlendirilir. Aktarım şartı bulunmayan düzenli yurt dışı aktarım yapılmaz.

• Tedarikçi ve veri işleyenlerle yapılan sözleşmelerde kişisel verilerin işlenme amacı, güvenlik tedbirleri, alt işleyen kullanımı, ihlal bildirimi, denetim hakkı, sözleşme sonunda iade/imha ve gizlilik hükümleri yer alır.

14. FİLYOS BELEDİYESİ HİZMETLERİNE GÖRE SAKLAMA ESASLARI

• Dilek & Şikâyet Formu, Başkana Mesaj, e-posta, KEP ve EBYS başvuruları; başvuru sonucu, ilgili birim cevabı, resmi yazışma ve denetim gerekleriyle birlikte değerlendirilir.

• Nikâh işlemleri, evlendirme memurluğu kayıtları, ücret/makbuz kayıtları, başvuru belgeleri ve iptal/iade kayıtları Evlendirme Yönetmeliği, nüfus vweb sitesi gelirleri mevzuatına göre saklanır.

• Halı saha ve düğün salonu tahsis kayıtları; rezervasyon, sözleşme, ödeme, güvenlik, olay/hasar ve iade süreçleriyle bağlantılı süreler boyunca saklanır.

• İmar, ruhsat, zabıta, işgaliye, pazar yeri, mühürleme, kaçak yapı, yol/kaldırım bakım-onarım ve saha tespit kayıtları; imar, ruhsat, kabahat, belediye gelirleri, tebligat ve dava zamanaşımı süreleriyle birlikte değerlendirilir.

• Sosyal yardım, sağlık/İSG ve özel nitelikli veri içeren kayıtlar; ilgili kamu hizmeti ve kanuni yükümlülükle sınırlı saklanır, erişim yetkisi dar tutulur ve gereksiz kopya oluşturulmaz.

• Meclis kararları, ilan/askı süreçleri, duyurular ve kamuya açık karar kayıtları; şeffaflık, arşiv ve mevzuat gerekleri kapsamında saklanır. Kamuya açıklanacak içeriklerde gereksiz kişisel veri maskeleme ilkesi uygulanır.

15. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK EK İDARİ TEDBİRLER

• Birim bazlı kişisel veri envanteri, saklama süresi, kayıt ortamı, yetkili kullanıcı, alıcı grubu ve imha yöntemi her yıl gözden geçirilir.

• Gereksiz kişisel veri toplanmasını önlemek için formlar sadeleştirilir; aynı verinin farklı birimlerde mükerrer tutulması azaltılır.

• Fiziki arşivlerde anahtar teslim kayıtları, yetkili personel listesi, dosya ödünç alma/iade kayıtları ve ziyaretçi erişim kontrolleri uygulanır.

• Elektronik arşiv ve dosya alanlarında klasör yetkilendirmesi, erişim logu, yedekleme, versiyon kontrolü ve imha planı birlikte işletilir.

• Denetim, teftiş, soruşturma, dava veya resmi kurum talebi bulunan dosyalar için imha askı kararı kayıt altına alınır; süreç tamamlandığında saklama süresi yeniden değerlendirilir.

16. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK EK TEKNİK TEDBİRLER

• Kritik sistemlerde düzenli yedekleme ve geri dönüş testi yapılır; yedeklerin erişim yetkisi, saklama süresi ve imha yöntemi ana veriyle birlikte tanımlanır.

• Kamera kayıt cihazları, web sitesi yönetim paneli, e-posta, EBYS, muhasebe/tahakkuk ve dosya paylaşım sistemlerinde yönetici hesapları sınırlı tutulur; MFA ve güçlü parola politikası uygulanır.

- Log kayıtları değiştirilemeyecek şekilde korunur; olay incelemesi dışında amaç dışı kullanılmaz. Log saklama süreleri 5651 ve bilgi güvenliği gerekliliklerine uyumlu belirlenir.
- Taşınabilir medya kullanımı zorunlu hallerle sınırlandırılır; şifreleme, virüs tarama, zimmet ve iade/imha kayıtları uygulanır.
- Özel nitelikli kişisel veri içeren dosyalar şifreli, erişimi kısıtlı, etiketli ve mümkünse ayrı saklama alanında tutulur.

17. DENETİM VE EĞİTİM

- Saklama ve imha uygulamaları yılda en az bir kez denetlenir; eksiklikler düzeltici/önleyici faaliyet planına alınır. Denetimlerde veri envanteri, fiziki arşiv, elektronik klasörler, kullanıcı yetkileri, tedarikçi sözleşmeleri, kamera kayıt süreleri ve çerez tercih kayıtları kontrol edilir.
- Yeni başlayan personele oryantasyon kapsamında, mevcut personele periyodik olarak saklama, arşiv, güvenli imha, veri minimizasyonu, özel nitelikli veri güvenliği ve ihlal bildirimi eğitimi verilir.
- Eğitim katılım kayıtları, içerik versiyonu, tarih, katılımcı listesi ve ölçme/değerlendirme sonuçlarıyla birlikte saklanır.

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