



TARİH	22.09.2026
DOKÜMAN KODU	PPT-02
VERSİYON	V01
KURUM	DENİZLİ BOZKURT BELEDİYESİ
DETSİS / VKN	64553832 / 1620049750
İLETİŞİM	kvkk@denizlibozkurt.bel.tr / +90 (258) 831 50 10
KEP	bozkurtbelediyeaskanligi@hs01.kep.tr
WEB SİTESİ / ADRES	www.denizlibozkurt.bel.tr / Mehmetçik Mahallesi Muzaffer Arıcı Caddesi No:8, 20370 Bozkurt/Denizli
DOKÜMAN TÜRÜ	POLİTİKA PROSEDÜR VE TALİMAT

Kişisel Veri Saklama ve İmha Politikası

1 Amaç

Bu doküman, Bozkurt Belediye Başkanlığının ("Belediye veya Veri Sorumlusu") gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Belediyemizin görev, misyon, vizyon ve temel ilkeleri doğrultusunda; Belediyemizin süreç ve faaliyetlerinde yer alan tüm vatandaşlarımıza, çalışanlarımıza, çalışan adaylarımıza, işveren ve ihale adaylarımız ile çalışanlarına, tedarikçilerimiz ile çalışanlara, bünyemizde staj yapan stajyerlerimize, paydaş katılımcılarımıza, vergisel ve maddi mükelleflerimize ve ilgili kişilere ait kişisel verilerin; T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun"), Belediyemize ait mevzuat ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Belediye tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

2 Kapsam

Belediyemizin süreç ve faaliyetlerinde yer alan tüm vatandaşlarımıza, çalışanlarımıza, çalışan adaylarımıza, işveren ve ihale adaylarımız ile çalışanlarına, tedarikçilerimiz ile çalışanlarına, bünyemizde staj yapan stajyerlerimize, paydaş katılımcılarımıza, vergisel ve maddi mükelleflerimize ve ilgili kişilere ait kişisel veriler bu Politika kapsamında olup belediyenin sahip olduğu ya da belediye tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

3 Hukuki Dayanak

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
- Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
- Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik
- Kurul kararları ve yayımlanan rehberler

4 Tanımlar ve Kısaltmalar

KAVRAM	AÇIKLAMA
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu.
Kurul	Kişisel Verileri Koruma Kurulu.
Kurum	BOZKURT BELEDİYE BAŞKANLIĞI
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 Roller ve Sorumluluklar

Rol	Temel sorumluluk
Üst yönetim	Politikayı onaylar, kaynak sağlar ve önemli risk kararlarını verir.
KVKK koordinasyon sorumlusu	Envanter, aydınlatma, başvuru, eğitim, ihlal ve güncelleme çalışmalarını koordine eder.
Birim yöneticileri	Birim süreçlerinin envanterle uyumunu ve çalışanların kurallara uymasını sağlar.
Bilgi İşlem	Teknik güvenlik, erişim, log, yedekleme ve olay müdahale kontrollerini yürütür.
Tüm kullanıcılar	Yetkilerini amacıyla sınırlı kullanır, gizliliği korur ve olayları gecikmeden bildirir.
Tedarikçiler ve veri işleyenler	Wözleşme, protokol ve taahhütlerde yer alan veri güvenliği yükümlülüklerine uygun hareket eder.

6 Uygulama Kuralları

- Saklama süresi; mevzuat, kamu arşiv planı, hizmetin tamamlanması, zamanaşımı ve ispat ihtiyacı birlikte değerlendirilerek belirlenir.
- İşleme şartları ortadan kalkan veriler ilk periyodik imha döneminde silinir, yok edilir veya anonim hâle getirilir.
- Periyodik imha kontrolü altı ayı aşmayacak aralıklarla yürütülür.
- İmha işlemleri yöntem, kapsam, tarih, sorumlu ve onay bilgisiyle kayıt altına alınır; kayıtlar en az üç yıl saklanır.
- Yedeklerde bulunan veriler geri yükleme döngüsü içinde erişilemez hâle getirilir veya güvenli biçimde üzerine yazılır.

7. İlgili Kişi Grupları ve Veri Kategorileri

Vatandaşlar, başvuru sahipleri, çalışanlar, aday çalışanlar, stajyerler, eski çalışanlar, meclis/encümen üyeleri, muhtarlar, tedarikçi/alt işveren çalışanları, ziyaretçiler, halı saha/düğün salonu kullanıcıları, belediye hizmet 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, belediye hizmet ve başvuru bilgileri.

8. Kayıt Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (e-posta, Web) Yazılımlar (Belediye Otomasyonu, EBYS) Çıkarılabilir Bellek (Harddisk, DVR Kayıt Cihazı) Belediye Bilgisayarı (Masaüstü, Dizüstü) Bilgi Güvenliği Cihazları (Antivürüs Programı, Firewall, Log Kayıtları,)	Kağıt Yazılı, Basılı, Görsel Ortamlar (Afiş, Pano)

Kayıt ortamı değiştiğinde envanter, saklama süresi ve imha yöntemi güncellenir.

9. Saklamayı Gerektiren Hukuki 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 uyumsuzluk ihtimali, arşiv yükümlülüğü ve veri minimizasyonu ilkesi birlikte değerlendirilir.

10. Saklama Süresi Belirleme Esasları

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 gereklilikleriyle 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 uyumsuzluk, denetim, soruşturma veya resmi talep halinde imha işlemi ilgili dosya bakımından askıya alınabilir.

11. İmha Yöntemleri

- 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 maskeleyme, toplulaştırma, örnekleme, genelleştirme, kayıt/değişken çıkarma, gürültü ekleme, k-anonimlik, l-çeşitlilik ve t-yakınlık gibi yöntemler kullanılabilir.
- 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. Aydınlatma Başvuru ve Hak Kullanım Kayıtları

- Aydınlatma metinleri, başvuru formları, açık rıza metinleri, ilgili kişi başvuru formları, başvuru değerlendirme yazıları ve cevap kayıtları, ispat yükümlülüğü ve hukuki uyumsuzluk 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. Aktarım ve Yurtdışı Aktarım Kayıtları

- Kişisel verilerin yetkili kamu kurumlarına, bankalara, KEP/e-posta/elektronik bildirim 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, elektronik bildirim/e-posta veya bulut altyapısı nedeniyle yurt dışına aktarım ihtimali varsa KVKK m.9 kapsamında uygun mekanizma değerlendirilir.
- 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. Belediye Hizmetlerine Göre Saklama Esasları

- İletişim ve çözüm merkezi kanalları, e-posta, KEP ve EBYS başvuruları; başvuru sonucu, ilgili birim cevabı, resmi yazışma ve denetim gerekleriyle birlikte değerlendirilir.
- Evlendirme İşlemleri işlemleri, evlendirme memurluğu kayıtları, ücret/makbuz kayıtları, başvuru belgeleri ve iptal/iade kayıtları Evlendirme Yönetmeliği, nüfus ve web sitesi gelirleri mevzuatına göre saklanır.

- Kurs, Havuz; 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.
- Vatandaş destek, 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 maskeleyme ilkesi uygulanır.

15. Denetim ve Eğitim

- 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 bildirim 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 bildirim, parola ve güvenli aktarım eğitimleri verilir.
- Tedarikçi ve veri işleyen sözleşmeleri, kişisel veri güvenliği, gizlilik, alt işleyen, ihlal bildirim, 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.

7 Kayıt Denetim ve Güncelleme

Uygulama kayıtları denetime elverişli biçimde saklanır. Süreç, sistem, mevzuat veya Kurul kararı değiştiğinde doküman ve envanter birlikte gözden geçirilir. En az yılda bir uygunluk kontrolü yapılır.

8 Yürürlük

Bu doküman 22.09.2026 tarihinde yürürlüğe girer. Uygulama sorumluları belgenin güncel sürümünü kullanır.

Hazırlayan

Kontrol eden

Onaylayan

