KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

KURUM	SARIZ BELEDİYE BAŞKANLIĞI
DOKÜMAN KODU	PPT-02
SÜRÜM / TARİH	V04 / 11.11.2026
RESMÎ WEB SİTESİ	https://sariz.bel.tr/

1. AMAÇ, KAPSAM VE YÜRÜRLÜK

Bu politika, Sarız Belediye Başkanlığının 6698 sayılı Kanun kapsamında işlediği kişisel verileri hangi gerekçelerle ve ne kadar süreyle muhafaza ettiğini, saklama sebebi sona erdiğinde hangi yöntemlerle imha edeceğini ve her işlem için nasıl kayıt tutulacağını belirler. Fiziksel dosyalar, e-posta, elektronik belge yönetimi, mali kayıtlar, personel dosyaları, başvuru/dilekçeler ve diğer veri kayıt ortamları kapsamdadır. Belge Belediye yetkili yönetiminin onayıyla yürürlüğe alınır.

2. HUKUKİ DAYANAK VE GENEL İLKELER

• 6698 sayılı Kanun m.4 uyarınca kişisel veriler doğru ve gerektiğinde güncel, belirli-açık-meşru amaçlarla, amaçla bağlantılı, sınırlı, ölçülü ve gerekli süre kadar saklanır.

• 6698 sayılı Kanun m.7 ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik gereğince işleme şartı sona eren kayıtlar imha edilir.

• Belediye kayıtlarının kanuni saklama çerçevesi somut faaliyete göre 5393 sayılı Belediye Kanunu, 5018 sayılı Kanun, 213 sayılı Vergi Usul Kanunu, 657 sayılı Kanun, 4857 sayılı Kanun, Evlendirme Yönetmeliği, Devlet Arşiv Hizmetleri Hakkında Yönetmelik ve ilgili diğer özel düzenlemelerle değerlendirilir.

• Tek bir genel saklama süresi tüm veri kayıtlarına uygulanmaz; asıl belirleme kişisel veri işleme envanteri ve dayanak kayıt tablosunda yapılır.

3. TANIMLAR VE SORUMLULAR

• Saklama: Kişisel verinin belirli hukuki sebep ve amaç için güvenli ortamda muhafazası. İmha: Silme, yok etme veya anonim hâle getirme. İlgili kullanıcı: Görevi kapsamında veriye erişen yetkili kişi.

• Üst yönetim: Politikanın onayı, uygulama kaynakları ve yıllık gözetim. KVKK koordinasyonu: Envanter, hukukî saklama dayanağı, dönemsel imha takvimi ve tutanakların koordinasyonu.

• Yazı İşleri ve arşiv: Gelen/giden resmî evrak, kurumsal arşiv ve devlet arşivi yükümlülüklerinin takibi. İnsan Kaynakları: Özlük ve iş sağlığı kayıtları. Mali Hizmetler: Vergi, tahakkuk, muhasebe ve ödeme kayıtları.

• Bilgi İşlem: Elektronik silme, yedekleme döngüsü ve kayıt ortamı kontrolleri. Süreç sahipleri: Her kaydın gerçek saklama nedeni, erişim sınırlaması ve imha kararının belgeye dayalı doğruluğu.

4. KAYIT ORTAMLARI VE SAKLAMA ESASLARI

• Elektronik ortam: Kurumsal EBYS/dosya ve e-posta sistemleri, mevzuata tabi mali kayıtlar, yetkili uygulama veri tabanları, loglar ve güvenli yedekler.

• Fiziksel ortam: Özlük dosyaları, başvuru/dilekçeler, nikâh/ruhsat/imar evrakı, sözleşmeler, ihale ve mali belgeler ile imha tutanakları.

• Taşınabilir ortamlar: İzinli kurumsal cihaz veya şifreli taşıyıcıda tutulan geçici iş kopyaları; kalıcı ayrı bir arşiv olarak kullanılmaz.

• Her kayıt türünde veriyi toplama sebebi, yetkili erişim, ilgili mevzuat süresi ve varsa yedekleme yöntemi belirlenir; yedekler de imha planına dâhildir.

SÜREÇ BAZINDA SAKLAMA DAYANAĞI KONTROLÜ

Kayıt grubu	Saklama ve özel mevzuat değerlendirmesi	İmha ve sorumlu birim
Vatandaş başvurusu / dilekçe	3071 sayılı Kanun, resmî yazışma ve kamu arşiv yükümlülükleri; başvuruya özgü süre	Yazı İşleri / ilgili müdürlük
Personel / özlük / İSG	657, 4857, 6331, 5510 sayılı düzenlemelerin uygulanabilir hükümleri	İnsan Kaynakları / ilgili sağlık yetkilisi
Vergi / tahakkuk / tahsilat	213 sayılı Vergi Usul Kanunu, 1319 sayılı Emlak Vergisi ve 2464 sayılı Belediye Gelirleri Kanunu	Mali Hizmetler
İhale / sözleşme / hakediş	4734, 4735 ve 5018 sayılı Kanunlar ile kamu arşiv yükümlülükleri	İhale birimi / Mali Hizmetler
İmar / ruhsat / evlendirme	3194 sayılı İmar Kanunu, ilgili ruhsat/evlendirme düzenlemeleri ve arşiv sınıflaması	İlgili hizmet müdürlüğü
Kamera / ziyaretçi / teknik log	Somut kayıt amacı ve hukuki sebep, risk analizi ve belirlenmiş kurum içi kayıt düzeni	İdari birim / Bilgi İşlem

5. SAKLAMA SÜRESİNİN BELİRLENMESİ

• Her kişisel veri kategorisi için işlem amacı, veri sorumlusu birimi, dosya türü, hukuki dayanak, süreyi başlatan olay, saklama bitişi ve imha yöntemi envanterde kaydedilir.

• Kanunda açık saklama süresi varsa bu süre uygulanır; süre yoksa hizmetin yürütülmesi, ispat ve hakların korunması için gerekli en kısa makul süre belgeli risk değerlendirmesiyle belirlenir.

• Süre dolduğunda kanuni arşiv zorunluluğu, yargısal uyuşmazlık veya yetkili makam talebi olup olmadığı kontrol edilir. Devam eden haklı gerekçe yalnız ilgili kayıt ve gerekçe süresiyle sınırlanır.

• Çerez, IP/log, CCTV, ziyaretçi ve iş başvurusu gibi birbirinden farklı kayıtlara aynı süre otomatik uygulanmaz; ilgili ortam için ayrı ve doğrulanmış süre belirlenir.

6. İMHA GEREKTİREN DURUMLAR

Kişisel veri işleme amacının ortadan kalkması; dayanak mevzuatın değişmesi; işleme şartının bulunmaması; saklama süresinin dolması; ilgili kişinin Kanun m.11 ve m.13 kapsamında haklı talebi veya işleme sebebinin başka şekilde sona ermesi hâllerinde ilgili kayıt için silme, yok etme veya anonim hâle getirme kararı verilir. İmha öncesinde diğer kanuni saklama nedenlerinin bulunmadığı kontrol edilir.

7. İMHA YÖNTEMLERİ

• Fiziksel evrak: Geri döndürülemeyecek biçimde güvenli parçalama/yok etme; dış hizmet varsa teslim ve imha tutanağıyla izleme.

• Elektronik veri: Kayıt ortamına ve verinin özelliğine uygun güvenli silme veya geri getirilemez yok etme; yetkili sistem yöneticisinin kayıtlı onayıyla işlem.

• Yedekler: Canlı sistemden silinen verilerin yedeklerdeki kopyaları teknik yedek döngüsü ve geri yükleme prosedürüyle birlikte yönetilir; geri yükleme yapılırsa silme kararı yeniden uygulanır.

• Anonim hâle getirme: Kişi belirlenmesini teknik ve idari olarak mümkün kılmayacak yöntemle, başka verilerle birleştirme riski dikkate alınarak gerçekleştirilir. Sadece isim karartmak her durumda anonimleştirme sayılmaz.

8. PERİYODİK İMHA TAKVİMİ VE KAYITLAR

Saklama ve imha politikası hazırlama yükümlülüğü kapsamındaki veri sorumlularında periyodik imha aralığı ilgili Yönetmelik uyarınca altı ayı aşamaz. Belediye fiili imha dönemlerini yıllık kontrollü takvimde belirler. İmha işlemleri DG-07 Saklama Süresi ve İmha Karar Formu ile DG-08 Periyodik İmha Tutanakları üzerinden tarih, kayıt grubu, gerekçe, yöntem, işlemci, kontrol ve kanıt bilgisiyle kayıt altına alınır. İmha kayıtları ilgili Yönetmelik gereği diğer hukuki yükümlülükler saklı olmak üzere en az üç yıl saklanır.

9. GÜVENLİK, DELİL KORUMA VE İSTİSNALAR

• Kayıtlar görevle sınırlı erişim, gerekli hesap/klasör yetkileri, fiziksel kilit ve uygun teknik güvenlik tedbirleriyle korunur. Kurumda uygulanıp uygulanmadığı doğrulanmamış denetim, sızma testi, şifreleme veya otomatik imha tedbiri mevcutmuş gibi raporlanamaz.

• Ve-ri güvenliği ihlali halinde olay kayıtları delil bütünlüğüyle korunur; ihlal müdahale prosedürü işletilir.

• Açık dava, soruşturma, resmi denetim veya kanunen muhafaza gerektiren durumlarda yalnız ilişkili kayıt geçici imha askısına alınır; gerekçe ve gözden geçirme tarihi kayıt altına alınır.

10. EĞİTİM, İZLEME VE GÖZDEN GEÇİRME

Personel yetkileri, veri kategorileri, saklama süreleri ve imha tutanakları süreç sahipleri tarafından düzenli kontrol edilir. Politika yılda en az bir kez ve hizmet/mevzuat/altyapı değişikliklerinde gözden geçirilir. Belediye yetkili makamı tarafından onaylanıp doküman siciline işlendiğinde güncel sürüm yürürlüğe girer.

11. İLGİLİ BELGELER VE KAYNAKLAR

• 6698 sayılı Kanun m.4, m.7, m.11, m.12 ve m.13.

• Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik; Devlet Arşiv Hizmetleri Hakkında Yönetmelik.

• Kişisel Veri İşleme Envanteri, Kişisel Veri İhlali Müdahale Prosedürü, Yetkilendirme Prosedürü, DG-06 Envanter Analiz Formu, DG-07 Saklama Süresi Karar Formu ve DG-08 İmha Tutanağı.

DOKÜMAN KONTROL VE ONAY

Hazırlayan	Kontrol Eden	Onaylayan
KVKK Koordinasyonu	Yazı İşleri / İlgili Süreç Sahibi	Belediye Başkanlığı
Ad Soyad / Tarih / İmza:	Ad Soyad / Tarih / İmza:	Ad Soyad / Tarih / İmza:

REVİZYON NO: V04 | TARİH: 11.11.2026 | Konu: Saklama süresi ve imha kayıtlarının hizmet bazında güncellenmesi.