SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Bu politikanın amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun)'na uyum kapsamında, Bodrum Belediyesi ("Belediye") tarafından işlenen kişisel verilerin işlendikleri amaç için gerekli olan azami süreyle saklanması ve imha edilmesine ilişkin usul ve esasların, kurum içi kontrol ve önlemlerin, işleyiş kurallarının ve sorumlulukların belirlenmesidir

2. KAPSAM

Bu politika hükümleri, Belediye tarafından kişisel verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen çalışan adayı, çalışan, meclis-encümen üyeleri, ilişkide olunan diğer kurum ve kuruluş yetkilileri, ticari ilişki içinde olunan tedarikçi yetkilileri, muhtar ve kişisel verisi Belediye tarafından işlenen tüm vatandaşlar hakkında uygulanır. İşbu Politika "Kişisel Veri İşleme Envanteri"ne uygun olarak hazırlanmıştır.

3. TANIMLAR

Bu politikada yer alan önemli tanımlar aşağıda belirtilmiştir.

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Ayıklama ve İmha Komisyonu	Belediye'nin arşiv hizmet ve faaliyetlerinin düzenlenmesinde görev alan personelleri
Bilgi Güvenliği Politikası	Bilgi İşlem Müdürlüğünün yayınladığı Bilgi ve Sistem Güvenliği Politikaları Yönergesi
Doğrudan tanımlayıcılar	Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılar
Dolaylı tanımlayıcılar	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılar
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kanun/KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu

Karartma	Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemler
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel Verilerin Silinmesi	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
Manyetik Bant	Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlar
Manyetik Disk	Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlar
Maskeleme	Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemler

Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
Veri işleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Koruma Komisyonu	Belediye'nin Veri Koruma Komisyonu'nu ifade eder.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi

4. SORUMLULUK

İşbu Politika Veri Koruma Komisyonu tarafından onaylanıp yürürlüğe girmiştir. Veri Koruma Komisyonu Belediye'nin tüm çalışanlarının işbu Politika'yı okumalarını sağlar.

Tüm Belediye çalışanları, görevlerini işbu Politika'ya ve ilgili tüm politika, prosedür ve mevzuata uygun olarak yerine getirmekten sorumludur.

5.KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, Belediye tarafından işbu Politika kapsamında düzenlenen aşağıdaki kayıt ortamlarında başta Kanun hükümleri olmak üzere ilgili mevzuata uygun olarak ve veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

a) Kâğıt ortamı
b) Hard Diskler
c) Mobil cihazlar
d) Program/Yazılım/Uygulama/Sunucu

Kullanılan Program/Yazılım/Uygulama	**Açıklama**	**Veri Tabanı Lokasyonu**	**Yetkilendirme**
Saysis	Belediye'nin kullandığı otomasyon programı	Belediye sunucuları	Var
E-belediye	İçişleri bakanlığının çevrimiçi sistemi	Belediye dışı-Yurt içi	-
Server	Güvenlik duvarı ile korunan Belediye sunucuları	Belediye sunucuları	Var
Web yönetim paneli	Güvenlik duvarı ile korunan Belediye'nin web sitesinin yönetim paneli	Belediye dışı-Yurt içi	Var
Tegsoft	Çağrı merkezi programı	Belediye sunucuları	Var
Personel takip programı	Belediye'nin kullandığı personel takip program	Belediye sunucuları	Var

Netcad Server	GIS programı	Belediye sunucuları	Var
Mobilpark SMS	Belediye'nin SMS'lerinin atıldığı platform. Online servis olarak kullanılmaktadır. Güvenlik BTK tarafından denetlenmektedir.	Belediye dışı-Yurt içi	Var
OSKA hakediş programı	Fen İşleri Müdürlüğü tarafından kullanılan hakediş programı	Belediye sunucuları	Var
Ekap	Kamu İhale Kurumunun servisi	Belediye dışı-Yurt içi	-
AssistCRM	Whatsapp şikayet hattının kullanıldığı firma	Belediye dışı-Yurt içi	-
Çözüm Masası	Saysis otomasyon programının bir modülü	Belediye sunucuları	Var

6. KİŞİSEL VERİLERİN İMHASI

Belediye tarafından toplanan kişisel veriler, Kanun'un 5. ve 6. maddelerinde belirtilen işleme şartlarına uygun olarak Kişisel Verilerin İşlenmesi ve Korunması Politikası'nda belirtilen amaçlar dahilinde işlenmekte ve Envanter'de belirtilen amaçlarla saklanmaktadır:

Belediye'nin faaliyetleri çerçevesinde işlenen kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 5393 sayılı Belediyeler Kanunu,
- 657 sayılı Devlet Memurları Kanunu,
- 4743 sayılı Kamu İhale Kanunu,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 4982 sayılı Bilgi Edinme Kanunu,
- 3017 sayılı Dilekçe Hakkının Kullanılması Kanunu,
- 5115 sayılı Kimlik Bildirme Kanunu,
- İlgili diğer kanunlar ve ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanır.

Kanun ve ilgili diğer kanun ve ikincil düzenlemelerin hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya İlgili Kişinin talebi üzerine Belediye tarafından silinir, yok edilir veya anonim hâle getirilir. Buna göre;

- Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması,
- Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,

- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olduğunun tespit edilmesi,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, İlgili Kişinin rızasını geri alması,
- İlgili kişinin, Kanun'un 11. maddesinin 1. fıkrasının (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun Belediye tarafından kabul edilmesi,
- Belediye'nin, İlgili Kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikayette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

gibi hallerde kişisel verilerin silinmesi, yok edilmesi ya da anonim hâle getirilmesi sağlanır.

7. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEDBİRLER

Belediye tarafından kişisel verilerin, hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alınır; Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimlerin yapılması sağlanır. Belediye bünyesinde alınmakta olan idari ve teknik tedbirler aşağıda listelenmiştir;

7.1 İDARİ TEDBİRLER

a) Kişisel verilerin hukuka aykırı işlenmesinin önlenmesi (Aydınlatma-Açık Rıza- Taahhüt))
b) Kişisel verilerin güvenli bir şekilde muhafazasının sağlanması
c) Kişisel verilere hukuka aykırı erişilmesinin önlenmesi
d) Kişisel verilerin özel nitelikli kişisel veri olup olmadığının tespiti
e) Kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması için Belediye içi eğitimin tasarlanması, yapılması ve belgelenmesi
f) Veri sorumlusu nezdinde çalışanların kişisel veri güvenliğine ilişkin rol ve sorumluluklarının, görev tanımlarında belirlenmesi ve bunun çalışan tarafından kabul edildiğinin tespiti, Çalışanların bu konudaki rol ve sorumluluklarının farkında olmasının sağlanması için devamlı eğitim ve denetim yapılması
g) Politikalara uyulmaması durumlarına ilişkin yaptırımların belirlenmesi ve disiplin süreçlerinin hazırlanması, yürürlüğe sokulması ve uygun şekilde duyurulması
h) Politika ve prosedür değişikliklerin çalışanlara duyulması ve duyuruların belgelenmesi
i) Çalışanların, kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerini güncel tutmalarının sağlanması, periyodik hatırlatmalar gibi yöntemlerle devamlılığın sağlanması için uygulama/ prosedürler geliştirilmesi
j) Veri güvenliği prosedürleri kapsamında düzenli kontrol yapılması
k) Veri güvenliği prosedürleri kapsamında yapılan kontrollerin belgelenmesi
l) Güvenlik konusunda geliştirilmesi gereken hususların belirlenmesi
m) Alınan kişisel verilere ihtiyaç olup olmadığının değerlendirilmesi, işleme amacı için ihtiyaç duyulan veriden fazlasının talep edilmemesi ve işlenmemesini teminen süreçler bazında gerekli çalışmaların tamamlanması; yeni proje ve süreçlerin bu kapsamda tasarlanması
n) Kişisel veri işleme envanterinde yer alan "İmha Süreleri"ne uyulmasının sağlanması, periyodik olarak kontrol edilmesi
o) Veri işleyenden, veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen işleme amaç ve kapsamına uygun ve mevzuata uyumlu şekilde hareket edeceğine dair beyan ve garanti alınması -Veri Sorumlusundan Veri İşleyene Aktarım Politikasının imzalatılması

7.2 TEKNİK TEDBİRLER

Belediye, görevi ve konumu nedeniyle sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında bilgi çağı gereklerine uygun olarak tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmek amaçlarıyla Bilgi Güvenliği Politikası hazırlamış ve yürürlüğe koymuştur. Kişisel Verilerin saklanmasında Bilgi Güvenliği Politikası'nın ilgili hükümleri dikkate alınmaktadır. Bu hükümlere ek olarak Kurul tarafından yayınlanan "Kişisel Veri Güvenliği Rehberi"nde yer alan teknik tedbirlerden aşağıda sıralananlar alınmaktadır.

a) Güvenlik duvarı ve ağ geçidi olup olmadığının kontrol edilmesi, yoksa kurulması
b) Yazılım ve donanımların kurulum ve yapılandırma işlemine tabi tutulması
c) Kullanılmayan yazılım ve servislerin silinmesi
d) Yama yönetimi ve yazılım güncellemeleri
e) Yazılım ve donanımların düzgün çalışıp çalışmadığına ilişkin düzenli kontrollerin yapılması
f) Sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi
g) Erişim için güçlü şifre ve parolaların oluşturulması
h) Şifre girişi deneme sayısının sınırlandırılması
i) Düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması
j) İlişkileri kesilen çalışanların hesabının silinmesi ya da girişlerinin kapatılması
k) Sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması, düzenli taramaların yapılması ve bu ürünlerin güncel tutulması
l) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi
m) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi
n) Tüm kullanıcıların işlem hareketleri kaydının (log kayıtları gibi) düzenli olarak tutulması
o) Güvenlik sorunlarının mümkün olduğunca hızlı şekilde raporlanmasının sağlanması
p) Güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi ve bu sistemlerden gelen uyarılar üzerine harekete geçilmesi
q) Bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak zafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirme yapılması
r) Bilişim sistemine yönelik istenmeyen olaylarda delillerin toplanması ve güvenli bir şekilde saklanması
s) Elektronik ortamdaki ağ bileşenleri arasındaki erişimin sınırlandırılması veya bileşenlerin ayrılması
t) E-posta ya da posta ile aktarılacak kişisel verilerin dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi
u) Teknik destek için üçüncü kişilere gönderilen cihazlarda sadece arızalı parçaların gönderilmesi, geri kalan veri saklama ortamlarının sökülerek çıkartılması
v) Teknik destek için dışarıdan gelen üçüncü kişilerin kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için önlem alınması
w) Kişisel verilerin yedeklenmesi ve kişisel verileri kilitleyen kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için yedekleme stratejisi geliştirilmesi

7.3 YAZILIM/PROGRAM/UYGULAMALARIN KULLANIMI

İşbu Protokol'ün 5.maddesindeki tabloda yer alan kullanılan yazılım/program/uygulamaların güvenliği Bilgi İşlem Müdürlüğü tarafından gerçekleştirilen periyodik denetimler ile denetlenmektedir.

7.4 AKTARILAN VERİLERİN GÜVENLİĞİ VE İMHASI

Kişisel Verileri Belediye adına işleyen Veri İşleyenler'den, Belediye'nin talimatları doğrultusunda, sözleşmede belirtilen işleme amaç ve kapsamına uygun ve mevzuata uyumlu şekilde hareket edeceğine

dair beyan ve garanti alınmaktadır ve Veri İşleyen'in verilerin İmhası konusunda işbu Politika hükümlerine uyması sağlanmaktadır.

8. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINAN TEDBİRLER

8.1 KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirler Belediye tarafından alınmaktadır.

Kişisel verilerin silinmesi işleminde izlenen süreç aşağıdaki gibidir:

1. Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
2. Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
3. İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
4. İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Kişisel veriler saklandıkları kayıt ortamlarına uygun yöntemlerle silinir.

a) **Bulut ortamındaki veriler**, silme komutu verilerek silinir. İlgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmaması sağlanır.

b) **Kâğıt ortamında bulunan kişisel veriler,** karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

c) **Merkezi sunucuda yer alan ofis dosyaları**, işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması sağlanır. Bu işlemi gerçekleştiren kullanıcının, veri tabanı yöneticisinden farklı bir kişi olması sağlanır.

d) **Flash tabanlı saklama ortamlarındaki kişisel veriler**, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinir.

e) **Veri tabanlarında saklanan kişisel verilerin**, bulunduğu ilgili satırların veri tabanı komutları ile (Delete) silinmesi sağlanır. Bu işlemi gerçekleştiren kullanıcının, veri tabanı yöneticisinden farklı bir kişi olması sağlanır.

8.2 KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirler Belediye tarafından alınmaktadır.

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyalar tespit edilir ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerle tek tek yok edilir:

a) **Yerel sistemler üzerindeki verilerin** yok edilmesi için aşağıdaki yöntemler kullanılır:

- **De-manyetize etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemi.

- **Fiziksel yok etme:** Optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi işlemi.

- **Üzerine yazma**: Özel yazılımlar kullanılarak, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemi.

b) **Çevresel sistemler üzerindeki verilerin** yok edilmesi için aşağıdaki yöntemler kullanılır:

- **Ağ cihazları (switch, router vb.):** (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Manyetik bant:** Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.

- **Manyetik disk gibi üniteler:** Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.

- **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Optik diskler (CD, DVD vb.):** Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.

- **Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

c) **Kâğıt ve mikrofiş ortamlarındaki kişisel veriler**, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi sağlanır. Bu işlem gerçekleştirilirken veriler, kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür. Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre de-manyetize edilmesi, fiziksel olarak yok edilmesi ve üzerine yazma gibi yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

d) **Bulut ortamında yer alan kişisel veriler için,** bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi sağlanır.

e) **Arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin** yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

- Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması sağlanır.

8.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, İlgili Kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır.

Belediye tarafından uygulanacak anonim hale getirme yöntemleri belirlenirken, sahip olunan veri kümesine dair aşağıdaki özellikler dikkate alınarak, Kurum'un yayınladığı "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'nde yer alan yöntemlerinden uygun olanı kullanılır:

- Verinin niteliği,
- Verinin büyüklüğü,
- Verinin fiziki ortamlarda bulunma yapısı,
- Verinin çeşitliliği,
- Veriden sağlanmak istenen fayda / işleme amacı,
- Verinin işlenme sıklığı,
- Verinin aktarılacağı tarafın güvenilirliği,
- Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,
- Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,
- Verinin dağıtıklık/merkezilik oranı,
- Kullanıcıların ilgili veriye erişim yetki kontrolü,
- Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

8.3.1 Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri:

- Değişkenleri Çıkartma
- Kayıtları Çıkartma
- Bölgesel Gizleme
- Genelleştirme
- Alt ve Üst Sınır Kodlama
- Global Kodlama
- Örnekleme

8.3.2 Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri:

- Mikro Birleştirme
- Veri Değiş Tokuşu
- Gürültü Ekleme

8.3.3 Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler:

- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

9. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALAN PERSONEL

Kişisel verilerin işlenmesi, saklanması ve imhası süreçlerinde yer alan Belediye'nin tüm birimleri ve çalışanları, işbu Politika gereklerinin yerine getirilmesinden, Politika kapsamında alınan teknik ve idari tedbirlerin gereği gibi uygulanmasından ve kendi iş süreçlerinde ürettikleri verileri saklamak ve korumaktan sorumludurlar.

İmha işlemleri Veri Koruma Komisyonu ile birlikte Devlet Arşiv Hizmetleri Hakkında Yönetmeliğinin 19.maddesi uyarınca görevlendirilen Ayıklama ve İmha Komisyonu tarafından yürütülür.

10. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken;

a. İlgili veri kategorisinin işlenme amacı kapsamında Belediye'nin faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
b. İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve İlgili Kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,

c. İlgili veri kategorisinin işlenme amacına bağlı olarak Belediye'nin elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
d. İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
e. Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
f. Belediye'nin hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
g. Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,

dikkate alınır. Kişisel veri kategorilerinin işleme amaçlarına dayalı olarak işlenmeleri için gerekli olan azami muhafaza edilme sürelerinin, ilgili mevzuatta azami muhafaza edilme süresi öngörülmüşse, bu süreyi aşmayacak şekilde belirlenmesi gerekir.

Belediye Kişisel Veri İşleme Envanteri'ne uyumlu olarak belirlenen kişisel veri kategorisi bazında azami saklama sürelerini ve imha sürelerini gösteren tabloya aşağıda yer verilmiştir.

VERİ KATEGORİSİ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
Personel Özlük Dosyasının Oluşturulması ve Tutulmasına İlişkin Veriler	İş sözleşmesinin sona ermesini takiben 101 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesine İlişkin Veriler	Belediye sistemlerine kaydedilmesini takiben 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Meclis Kararları ve Yönetim Faaliyetlerine İlişkin Veriler	15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Personelin Yan Hakları ve Menfaatleri Süreçlerini Yürütmeye Yarayan ve Sözleşmenin İfasına İlişkin Veriler	Sözleşmenin sona erdiği tarihten itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Muhtemel bir uyuşmazlıkta hakkın korunması amacıyla işlenen veriler	Hukuki ilişkinin tabi olduğu zamanaşımı süresince	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde

Çalışanların sağlık verileri ve İş sağlığı ve güvenliği mevzuatı gereğince işlenen tüm verileri	İş Sağlığı ve Güvenliği mevzuatı gereğince işten ayrılma tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Belediye'ye Yönelik Talep ve Şikayetlere İlişkin Dilekçe Bilgileri	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Personelin Eğitim Seviyesini Yükseltmek Amacıyla Yapılan Çalışmalarda İşlenen Kişisel Veriler	Sözleşmenin sona erdiği tarihten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
İletişim faaliyetlerinin yürütülmesi esnasında elde edilen kimlik ve iletişim verileri	İhtiyaç Devam Ettiği Sürece	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Evlenme İşlemlerine ilişkin Veriler	30 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
İhale ve Sözleşme Süreçlerine İlişkin Veriler	Sözleşmenin sona erdiği tarihten itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
İlgili mevzuatta özel saklama süresi öngörülen diğer veriler	İlgili mevzuatta öngörülen saklama süresi boyunca-Ayıklama ve İmha Komisyonu tarafından belirlenir	Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde
Mevzuatta özel saklama süresi öngörülmeyen işlenen diğer veriler	İşleme amacı sona erdiğinde imha edilir/Devlet Arşivi'ne gönderilir ve imha edilir	İlk periyodik imha sürecinde

10.1 KİŞİSEL VERİLERİ RESEN SİLME, YOK ETME VEYA ANONİM HALE GETİRME SÜRELERİ

Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel veriler, Belediye tarafından resen altı aylık periyotlarda düzenli olarak silinir, yok edilir veya anonim hale getirilir. Kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde söz konusu işlemlerin uygulanması sağlanır.

İlgili kişisel veriler üçüncü kişilere aktarılmışsa bu durum veri aktarılan taraflara ve/veya Belediye'nin verdiği yetkiye dayanarak Belediye adına veri işleyenlere bildirilir ve bu kişiler nezdinde gerekli işlemlerin yapılması sağlanır.

10.2 KİŞİSEL VERİLERİ İLGİLİ KİŞİNİN TALEP ETMESİ DURUMUNDA SİLME VE YOK ETME SÜRELERİ

İlgili kişinin kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep etmesi halinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel veriler, Belediye tarafından en geç otuz gün içinde silinir, yok edilir veya anonim hale getirilir ve İlgili Kişiye bilgi verilir.
b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa bu durum veri aktarılan taraflara ve/veya Belediye'nin verdiği yetkiye dayanarak Belediye adına veri işleyenlere bildirilir ve bu kişiler nezdinde gerekli işlemlerin yapılması sağlanır.
c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Kanun'un 13. maddesi uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı İlgili Kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

10.3 SAİR HÜKÜMLER

Bu Politika çalışanlara Veri Koruma Komisyonu tarafından sunulacaktır.

Bu Politika yayınlandığı anda yürürlüğe girer.

Bu Politika'da her zaman değişiklikler yapılabilir. Yapılan değişikliklerin çalışanlara Veri Koruma Komisyonu tarafından bildirilmesi gerekmektedir.

EK.1 KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALAN PERSONEL

UNVAN	BİRİM	GÖREV TANIMI
Ayıklama ve İmha Komitesi	Ayıklama ve İmha Komitesi	Kişisel veri saklama ve imha politikası uygulama sorumlusu: periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
Birim/Departman Yöneticisi	Tüm Birimler	Görevlerine uygun olarak Politika'nın yürütülmesinden ve sorumlu olduğu birimde uygulanmasının sağlanmasından sorumludur.
Bilgi İşlem Müdürü	Bilgi İşlem	Kişisel verilerin güvenli bir şekilde saklanması, hukuka uygun olarak işlenmesi, erişilmesi ve imha edilmesine ilişkin teknik tedbirlerin alınmasından ve kişisel veri imha sürecinin yönetiminden sorumludur.
Veri Koruma Komisyonu	Veri Koruma Komisyonu	Politika'nın hazırlanması, yayınlanması, güncelliğinin sağlanması ve çalışanların politikaya uygun hareket etmesinden sorumludur.