

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1.1.Amaç

İşbu Kişisel Verileri Saklama ve İmha Politikası ("Politika"), "Veri Sorumlusu" (Tuğba Kayasu Avşar) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Bu kapsamda, Veri Sorumlusu (Tuğba Kayasu Avşar) çalışanlarının, çalışan adaylarının, hastalarının ve herhangi bir nedenle nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verilerinin, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve İşbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesi ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanması öncelik olarak belirlenmiştir.

1.2.Kapsam

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, veri sorumlusu Veri Sorumlusu tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.3 Kısaltmalar ve Tanımlar

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

Çalışan: Veri Sorumlusu çalışanları.

Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.

Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.

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 kişilerdir.

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.

Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

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 İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.

Kurul: Kişisel Verileri Koruma Kurulu

Periyodik İmha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.

Politika: Kişisel Verileri Saklama ve İmha Politikası

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

Veri Sorumluları Sicil Bilgi Sistemi: Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

VERBİS : Veri Sorumluları Sicil Bilgi Sistemi.

Yönetmelik: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.1. Sorumluluk Ve Görev Dağılımları

Tüm Veri Sorumlusu çalışanları, Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu çalışanlara aktif olarak destek verir.

3.1. KAYIT ORTAMLARI

Kişisel veriler, Veri Sorumlusu tarafından Tablo 1’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 1: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none">➤ Sunucular (Etki alanı, yedekleme,e-posta, veritabanı, web, dosya paylaşım, vb.)➤ Dijital Radyografi Programları➤ Yazılımlar (ofis yazılımları.)➤ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, antivirüs vb.)➤ Kişisel bilgisayarlar (Masaüstü, dizüstü)➤ Mobil cihazlar (telefon, tablet vb.)➤ Optik diskler (CD, DVD vb.)➤ Çıkarılabilir bellekler (USB, Hafıza Kart vb.)➤ Yazıcı, tarayıcı, fotokopi makinesi	<ul style="list-style-type: none">➤ Kağıt➤ Manuel veri kayıt sistemleri (anket formları, başvuru formları)➤ Yazılı, basılı, görsel ortamlar

4.1.Saklama ve İmha ile İlgili Açıklamalar

Veri Sorumlusu tarafından; çalışanlar, çalışan adayları ve hastalara ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.2. Saklamaya İlgili Açıklamalar

Kanunun 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6. maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Veri Sorumlusunun faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.3.Saklamayı Gerektiren Hukuki Sebepler

Veri Sorumlusu faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname,
- Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik,
- 3224 sayılı Türk Diş Hekimleri Birliği Kanunu,
- 29256 sayılı Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmelik,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret 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,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.4. Saklamayı Gerektiren İşleme Amaçları

Veri Sorumlusu, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- Ağız ve Diş Sağlığı Kuruluşu olarak verilen hizmeti yerine getirmek.
- Kurumsal iletişimi sağlamak.
- Kurum güvenliğini sağlamak
- İstatiksel çalışmalar yapabilmek.
- Muhasebe kayıtlarının tutulmasını sağlamak.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Veri Sorumlusu ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.5. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, durumlarında, Veri Sorumlusu tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

5. Kişisel Verilerin Saklanması ve İmhasına İlişkin Alınan Teknik ve İdari Tedbirler

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12. maddesiyle Kanunun 6/4 maddesi gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Veri Sorumlusu tarafından teknik ve idari tedbirler alınır.

5.1 Saklamaya İlişkin Teknik Tedbirler

Veri Sorumlusu tarafından, işlediği kişisel verilerin saklanması ile ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

Kişisel verilerin saklama alanlarına ilişkin teknolojik gelişmeler uyarınca çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal ve yazılımsal güvenlik sistemleri kurulur. Kişisel verilere yalnızca yetkili çalışanlar erişebilmektedir. Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir. Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa kurumsal e-posta adresiyle aktarılmaktadır. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmaktadır. Veri Sorumlusu çalıştığı 3. kişilerden de verilerin saklanmasında belirli standartların yerine getirilmesine ilişkin taahhütler talep eder. Bununla birlikte Veri Sorumlusu, kişisel verilerin kaybolmaması ve hukuk dışı kullanılmaması için gerekli önlemleri alır.

5.2 Saklamaya İlişkin İdari Tedbirler

Veri Sorumlusu tarafından, işlediği kişisel verilerin saklanması ile ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

Kişisel verilerin saklanması ile ilgili teknik ve idari riskler hakkında çalışanlar bilgilendirilerek farkındalık yaratılmakta, kişisel verilerin saklanması için üçüncü kişilerle iş birliği yapılması durumunda kişisel verilerin aktarıldığı şirketler ile yapılan sözleşmelere; kişisel verilerin aktarıldığı kişilerin, aktarılan kişisel verilerin korunması ve güvenli saklanması amacıyla gerekli güvenlik tedbirlerinin alınmasına ilişkin yükümlülük ve sorumluluklarını ortaya koyan hükümlere yer verilmektedir.

5.3 İmhasına İlişkin Teknik Tedbirler

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Veri Sorumlusu tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

5.4 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-2'de verilen yöntemlerle silinir.

Tablo 2: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca üzeri okunamayacak şekilde çizilerek / boyanarak / silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

5.5 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Veri Sorumlusu tarafından Tablo-3'te verilen yöntemlerle yok edilir.

Tablo 3: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemez şekilde yok edilir veya yakılarak imha edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

5.6 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, Veri Sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

5.7 İmha İlişkin İdari Tedbirler

Verilerin imhası Veri Sorumlusunun yalnızca yetkili çalışanları tarafından gerçekleştirilmektedir. Kişisel verilerin korunması ve imhası ile ilgili mevzuat dahilinde çalışanlara bilgi verilir. İş yeri dahilinde özellikle fiziksel imhaya ilişkin gerekli ekipman bulundurulur.

6. Saklama ve İmha Süreleri

Veri Sorumlusu tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak; Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;

Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi yerine getirilir.

Tablo 4: Verilerin Saklanması ve Yok Edilmesine İlişkin Süreler

Kişi Grupları	Saklama Süresi	İmha Süresi
Hastalar	10 Yıl	Saklama Süresinin Sona Ermesinden İtibaren 6 Ay
Çalışanlar	İşten Ayrılma Tarihinden Sonra 10 Yıl	Saklama Süresinin Sona Ermesinden İtibaren 6 Ay
İş Başvurusu Yapan Adaylar	Başvuru Süresinden İtibaren 10 Yıl	Saklama Süresinin Sona Ermesinden İtibaren 6 Ay
Yukarıdaki Veri Sahipleri Dışında İletişime Geçenler, Tedarikçiler, Tedarikçi yetkilisi/çalışanları	10 Yıl	Saklama Süresinin Sona Ermesinden İtibaren 6 Ay

Veri Kategorisi	Saklama Süresi	İmha Süresi
Kimlik,iletişim, özlük, hukuki işlem, müşteri işlem, finans ve muhasebe, mesleki deneyim, görsel ve işitsel kayıtlar, dernek-vakıf-sendika üyeliği bilgileri, sağlık bilgileri, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleri bilgisi	10 Yıl	Saklama Süresinin Sona Ermesinden İtibaren 6 Ay
Fiziksel mekan güvenliği	1 Ay	Saklama Süresinin Sona Erdiğinde
İşlem Güvenliği	2 Yıl	Saklama Süresi Sona Erdiğinde

7. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır.

8. POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, yasal zorunluluk durumlarında, mevzuat değişikliklerinde ve ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

9. POLİTİKANIN YÜRÜRLÜĞÜ

İşbu Politika, 07.12.2021 tarihinde yürürlüğe girer.