**1. Amaç:**
6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun 'una dayalı olarak çıkarılmış olan ve 30224 sayılı Resmî Gazete 'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5. ve 6. maddeleri gereği kişisel verilerin saklanması, imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen diğer yükümlülüklerin yerine getirilmesi için kurum genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

**2. Kapsam:** Bu politika, ..... Hastanesi çalışanlarını kapsamaktadır. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.

**3. Sorumluluklar:** Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde hastane nezdinde kişisel veri saklayan ve işleyen tüm personel sorumludur. Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür.

**4. Tanımlar ve Kısaltmalar:**
Anonim Hale Getirme; Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmedir.
İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.
Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri 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 envanteridir.
Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Özel Nitelikli Kişisel Veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerdir.
Periyodik imha: 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 getirmesi işlemidir.
Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

**5. Referans Dokümanlar:**
· 6698 Sayılı Kişisel Verilerin Korunması Kanunun 30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik

**6. Uygulama**
**6.1.** Kişisel Verilerin İmhası Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri (Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi maddeleri) kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir. Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

**Kişisel Verilerin Silinmesi Yöntemleri**

a. Kâğıt Ortamında Bulunan Kişisel Veriler: Karartma yöntemi kullanılarak silinmektedir.

b. Merkezi Sunucuda Yer Alan Ofis Dosyaları: İşletim sistemindeki silme komutu ile silinir.

c. Taşınabilir Medyada Bulunan Kişisel Veriler: Uygun yazılımlarla silinir.

d. Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir.

**Kişisel Verilerin Yok Edilmesi Yöntemleri**

a. Yerel Sistemlerde Bulunan Kişisel Veriler: De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir.

b. Çevresel Sistemlerde Bulunan Kişisel Veriler:

i. Ağ cihazları (switch, router vb.): a maddesinde belirtilen uygun yöntemler ile yok edilir.

ii. Flash tabanlı ortamlar: İlgili üreticinin önerdiği yöntemler ya da a maddesinde belirtilen yöntemler ile yok edilir.

iii. Manyetik bant: De-manyetize ederek ya da yakma, eritme gibi fiziksel yöntemlerle yok edilir.

iv. Sim Kart ve sabit hafıza kartları:a maddesinde de belirtilen uygun yöntemler ile yok edilir.

v. Optik diskler: yakma, küçük parçalara ayırma, eritme gibi fiziksel yöntemlerle yok edilir.

vi. Veri Kayıt Ortamı sabit olan çevre birimleri: a maddesinde belirtilen uygun yöntemler ile yok edilir.

c. Kâğıt Ortamlarında Bulunan Kişisel Veriler: Kâğıt imha makinaları kullanılarak yok edilir. Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan Kişisel veriler ise bulundukları ortama göre uygun yöntemlerle yok edilirler.

**Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri:**

Kişisel verilerin Anonim hale getirilmesi aşamasında, Kişisel Verileri Koruma Kurumu'nun yayınladığı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberinde gösterilen Kişisel Verilerin Anonim hale getirilmesi yöntemlerinden uygun olanı kullanılır. Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi bünyesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır. Verilerin imha edilmesinde Devlet Arşivleri Genel Müdürlüğünün yayınladığı saklama sürelerini belirten yönetmelik dikkatte alınır. Birim arşivinde, Kurum arşivinde veya Devlet Arşivlerinde olması gereken süreler dolduktan sonra imha edilmesinde sakınca olmayan veriler imha edilmektedir.

**Çok Paydaşlı Verilerin İmhası:** Merkezi Bilgi Sistemlerinde yer alan çok paydaşlı veri sahipliği bulunan kişisel verilerin imhasına yönelik karar alınması gerektiğinde ise Veri Sorumlusu Temsilcisi görüşü alınarak ve söz konusu kişisel veri hakkında işbu politikaya göre verinin saklanmasına veya silinmesine, yok edilmesine veya anonim hale getirilmesine karar verilir.

**6.2. Kişisel Verilerin Periyodik Gözden Geçirilmesi:** Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi birimler işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç altı aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu veya bir mahkemenin bildirimi üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır. Kişisel verilerin silinmesi, yok edilmesi veya 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. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde kanunun 4. (Kişisel Verilerin İşlenmesi) maddesindeki genel ilkeler ile 12. (Veri Güvenliğine İlişkin Yükümlülükler) maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmektedir.

**6.3. Kişisel Verilerin Saklanması Kişisel verilerin işlenme süreleri:**"Kişisel Veri İşleme Envanteri" içerisinde belirtilmiştir. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Saklama ve imha süreçleri yasal bir zorunluluk olmadığı sürece veri sahibinin talebi üzerine değişkenlik gösterebilir. Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kâğıt ortamındaki evraklar, CD, DVD ve USB gibi cihazların kullanılmadığı zamanlar da kilit altında tutulması, sadece yetkili personelin erişmesi ve giriş çıkışların kamera ile izlenmesi gibi fiziksel güvenliğe ilişkin önlemler alınmıştır. Dijital ortamda tutulan kişisel verilerin bulunduğu sunucular Hastane bilgi işlem odasında, gerekli güvenlik önlemleri alınmış şekilde saklanmaktadır. Kişisel Verilerin Güvenliğinin Sağlanması için alınan idari ve teknik tedbirler detaylı olarak Kişisel Verilerin Korunması ve İşlenmesi Politikasında yer almaktadır.