İÇİNDEKİLER

I. GİRİŞ

6698 Sayılı Kişisel Verilerin Korunması Kanunu ***("Kanun")*** 7 Nisan 2016 tarihinde yürürlüğe girmiş olup *"kimliği belirli veya belirlenebilir"* gerçek kişilere ***("ilgili kişi")*** ilişkin her türlü bilginin işlenmesine ilişkin düzenlemeleri içermektedir. Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş.***("Özel Vizyongöz Hastanesi")*** olarak Kanun gereği kişisel verilerin hukuka uygun olarak işlenmesi ve korunmasına azami önem veriyor, tüm planlama ile faaliyetlerimizde bu özenle hareket ediyoruz. Bu bilinçle Hastanemiz, kişisel verilerin korunması ve işlenmesi için tüm idari ve teknik tedbirleri almaktadır. Bu konunun en önemli ayağını ise işbu Kişisel Veri Saklama ve İmha Politikası ***("Politika")*** ile yönetilen; Hastalarımızın/Müşterilerimizin, Çalışan Adaylarımızın, Hastane Hissedarlarının, Hastane Yetkililerinin, Ziyaretçilerimizin, İşbirliği İçinde Olduğumuz Kurumların Çalışanlarının, Hissedarlarının, Yetkililerinin ve Üçüncü Kişilerin kişisel verilerinin korunması ve imhası oluşturmaktadır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Hastane tarafından bu doğrultuda hazırlanmış olan işbu Politikaya uygun olarak gerçekleştirilir.

1. POLİTİKA'NIN AMACI

İşbu Politika'nın amacını, Hastanemizce gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin usul ve esasların belirlenmesi oluşturmaktadır. Politika'nın amacı doğrultusunda, Hastanemiz tarafından gerçekleştirilen kişisel verilerin saklanması, korunması ve imhası faaliyetlerinde mevzuata tam uyumun sağlanması ile kişisel veri sahiplerinin özel hayat gizliliği ve veri güvenliği hakkının korunmasını hedeflenmekteyiz.

2. POLİTİKA'NIN KAPSAMI

İşbu Politika; Hastalarımızın/Müşterilerimizin, Çalışanlarımızın, Çalışan Adaylarımızın, Hastane Hissedarlarının, Hastane Yetkililerinin, Ziyaretçilerimizin, İşbirliği İçinde Olduğumuz Kurumların Çalışanlarının, Hissedarlarının, Yetkililerinin ve Üçüncü Kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen

tüm kişisel verilerine ilişkindir. Bu doğrultuda yukarıda sayılan kişisel veri sahiplerine Politika hükümlerinin tamamı uygulanabileceği gibi yalnızca bir kısım hükümleri de uygulanabilecektir.

3. TANIMLAR VE KISALTMALAR

İşbu Politika içerisinde yer alan tanımlara ek olarak aşağıda yer alan tanım ve kısaltmalar, yanlarında denk gelen açıklamayı ifade etmektedir.

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
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	Hastane personeli.
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.
Hizmet Sağlayıcı	Hastane ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
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.
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	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	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul	Kişisel Verileri Koruma Kurulu
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 verileri.
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme 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 İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Hasta/Müşteri	Hastanemizle herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Hastanemizin sunmuş olduğu ürün ve hizmetleri kullanan veya kullanmış olan gerçek kişilerdir
Çalışan Adayı	Hastanemize herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini Hastanemizin incelemesine açmış olan gerçek kişilerdir.
Hastane İş Ortağı, İş Ortaklarının Hissedarı, Yetkilisi, Çalışanı	Hastanemizin her türlü iş ilişkisi içerisinde bulunduğu gerçek kişiler ile Hastanemizin her türlü iş ilişkisi içerisinde bulunduğu gerçek ve tüzel kişilerde (iş ortağı, tedarikçi gibi) çalışan, hissedarları ve yetkilileri dâhil olmak üzere, tüm gerçek kişilerdir.
Potansiyel Hasta/Müşteri	Ürün ve hizmetlerimizi kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek

	kişilerdir.
Hastane Çalışanı	Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş. bünyesinde çalışan gerçek kişilerdir.
Hastane Hissedarı	Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş. hissedarı olan kişilerdir.
Hastane Yetkilisi	Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş. yönetim kurulu üyesi ve diğer yetkili kişilerdir.
Üçüncü Kişi	Hastane Çalışanları için hazırlanan Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş. Politikası kapsamına girmeyen ve bu Politika'da herhangi bir ilgili kişi kategorisine girmeyen diğer kişilerdir.
Ziyaretçi	Hastanemizin sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi herhangi bir amaç ile ziyaret eden tüm gerçek kişilerdir.

II. POLİTİKA ESASLARI

1. POLİTİKA'NIN VE İLGİLİ MEVZUATIN UYGULANMASI

İşbu Politika, yürürlükte bulunan mevzuat ile ortaya konulan kuralların Hastanemizin uygulamaları kapsamında somutlaştırılıp düzenlenmesiyle oluşturulmuştur. Bu kapsamda kişisel verilerin saklanması ve imhası konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Hastane'miz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir. Hastane olarak Kanun'da öngörülen yürürlük sürelerine uygun hareket etmek üzere gerekli sistem ve hazırlıkları yürütmekteyiz.

2. POLİTİKA'NIN YÜRÜRLÜĞÜ

Hastane'miz tarafından düzenlenerek 30.07.2018 tarihinde yürürlüğe giren Politika 02.01.2020 tarihinde güncellenmiştir.

3. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK VE DİĞER SEBEPLER

Hastane'miz tarafından kişisel veriler, **Özel Numune Sağlık Hizmetleri Ve Tic. A.Ş.** ***("Özel Vizyongöz Hastanesi")*** **Kişisel Verilerin İşlenmesi ve Korunması Politikası'nda** yer verilen amaçların gerçekleştirilmesi amacıyla mevzuat, sözleşme, talep ve isteğe dayalı hukuki sebepler çerçevesinde kanunlardan doğan sorumlulukları eksiksiz ve doğru bir şekilde yerine getirilebilmesi için toplanır ve Hastanemiz veya Hastanemiz tarafından görevlendirilen veri işleyenler tarafından işlenir.

a. Saklamaya İlişkin Esaslar

Kanun'un 10. maddesi gereği Hastanemiz, ilgili kişilere kişisel verilerinin hangi amaçlarla işlendiği bilgisini vermektedir. Hastanede, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler,

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,

- 6098 sayılı Türk Borçlar Kanunu,
- 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun,
- 6102 sayılı Türk Ticaret Kanunu,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname,
- Özel Hastaneler Yönetmeliği,
- Kişisel Sağlık Verileri Hakkında Yönetmelik,
- Hasta Hakları Yönetmeliği,
- Tıbbi Laboratuvarlar Yönetmeliği,
- Yataklı Tedavi Kurumları İşletme Yönetmeliği
- Sağlıkta Kalitenin Geliştirilmesi ve Değerlendirilmesine Dair Yönetmelik
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun,
- 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,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler ve sair mevzuat hükümleri

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

Hastane, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- Hizmetlerimizi sunabilmek ve bu hizmetlerin kalitesini artırabilmek,
- Kamu otoritelerince öngörülen ve/veya istisna olarak sayılan faaliyetleri yerine getirebilmek,
- Hastanemizin satış ve pazarlama faaliyetlerini yerine getirebilmek,
- Bilgi saklama, raporlama, bilgilendirme yükümlülüklerine uymak,
- İnsan kaynakları politikalarımızın en iyi şekilde planlanması ve uygulanmasını sağlamak,
- Ticari ortaklıklarımızın ve stratejilerimizin doğru olarak planlanması ve yürütülmesini sağlamak,
- Hastanemizin ve iş ortaklarımızın hukuki, ticari ve fiziki güvenliğinin teminini sağlamak,
- Hastanemiz kurumsal işleyişini sağlanmak,
- Hastane yerleşkelerini ziyaretlerde ilgili güvenlik ve meşru menfaatleri korumak,
- Hastanemizin ürün ve hizmetlerini sunmak,

- Ürün ve hizmete ilişkin iletişim kurmak,
- Pazarlama faaliyetlerinde kullanmak,
- Ürün/hizmet teklifi, modelleme, raporlama, risk izleme, mevcut veya yeni ürün çalışmaları ve potansiyel müşteri tespiti gibi Hastanemizin faaliyet konuları ile ilgili hizmetleri sunabilmek ve bu hizmetlerin kalitesini artırabilmek ve diğer faaliyetlerini yerine getirebilmek,
- Bilgilendirme yükümlülüklerine uymak,
- Hastanemiz internet sitesinde sunulan hizmetleri geliştirmek,
- Hastanemize talep ve şikâyetlerini iletenler ile iletişime geçmek,
- Hastanemiz internet sitesinde oluşan hataların gidermek,
- İnsan kaynakları süreçlerini yürütmek,
- Kurumsal iletişimi sağlamak,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- İstatiksel çalışmalar yapabilmek,
- Hastanemiz ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak,
- Çağrı merkezi süreçlerini yönetmek,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü,
- İş sözleşmesinin ifası için gerekli amacın yerine getirilmesi, özellikle;
  - Çalışanların izin onayı, bakiye izinlerin görüntülenmesi, izin düzenlemelerinin yapılması
  - Çalışanların işten çıkış işlemlerinin yapılması
  - Bordro işlemlerinin yapılmasının sağlanması
  - Çalışanlara maaş ödemelerinin yapılması
- İş Kanunu, İş Sağlığı ve Güvenliği Kanunu, Sosyal Güvenlik Kanunu ve ilgili mevzuat ile, diğer kanunlar ve mevzuat kapsamında gereklilikleri yerine getirmek amacıyla özellikle;
  - Personel özlük ve sağlık dosyasının oluşturulması
  - SGK bildirimleri, İŞKUR bildirimleri, karakol bildirimi ile teşvik ve yasal yükümlülük bilgilendirmesinin yapılması
  - Zorunlu bireysel emeklilik sigortası hesabı açılmasının sağlanması
  - Çalışanların giriş çıkış kayıtlarının kontrolü ve Ar-Ge için kamera kayıtlarının kapı giriş çıkış kayıtlarıyla olan eşleşmesinin tespit edilmesi
  - Ar-Ge için teşvik hesaplaması yapılması
  - İcra dosyalarına çalışanların maaş haciz kesintilerine ilişkin ödeme yapılması
  - İş kazasının yasal bildirimlerinin yapılması
  - İş sağlığı ve güvenliği işlemlerinin yapılması

- Mevzuat, ilgili düzenleyici kurumlar ve diğer otoritelerce öngörülen diğer bilgi saklama, raporlama, bilgilendirme yükümlülüklerine uymak
- Mahkeme kararlarının yerine getirilmesi

- Hasta/Müşteri sözleşmelerinin ifasından doğan gereklilik nedeniyle özellikle;
  - Hasta/Müşteri şikâyetlerinde müşterinin haklı/haksız ayrımının yapılması, müşteri memnuniyetinin arttırılması, müşteri ihtiyacının anlaşılması ve müşteri ile ilişkili süreçlerin iyileştirilmesinin sağlanması
  - Hastaya/Müşteriye hizmet kalitesinin değerlendirilmesi ve çalışanlara eğitim verilmesi
- Şirketin idaresi, işin yürütülmesi, Şirket politikalarının uygulanması amacıyla, özellikle;
  - Şirket çalışanlarının performanslarının takibi ve raporlanması
  - Çalışanlara masraf ödemelerinin yapılması
  - Çalışanlarla iletişimin sağlanması
  - Kendisine araç tahsis edilen veya kullandırılan çalışanın araba kullanmaya ehil olduğunun, ehliyetini herhangi bir nedenle kaybetmediğinin teyit edilmesi
  - Çalışana araç tedarik edilmesi ve park yeri ayarlanmasının sağlanması
  - Kartvizit basımının sağlanması
  - Kargo ve kurye aracılığıyla gelen paketlerin ilgili çalışana iletilmesinin sağlanması
  - Çalışanların güvenliği ve işin yürütülmesi için Şirket aracı kullanımının takip edilmesi
  - Servis ve seyahat organizasyonunun sağlanması
  - Çalışanın iş e-postasının oluşturulması
  - Çalışanlarla ilgili araştırma projeleri yürütülmesi
  - Çalışanların işe giriş ve çıkışlarının kontrolünün sağlanması
  - Çalışanların işe başvuru ve mülakatı süresince toplanan belgelerinin kayıt altına alınması
  - Kutlama amaçlı iletişimin sağlanması
  - Eğitim planlamasının yapılması, eğitimlerin raporlaması, eğitim sertifikalarının hazırlanması, gerçekleşen eğitimlere katılan çalışanların takip edilebilmesi, çalışanların aldıkları eğitimler sonucu gelişim süreçlerinin takip edilebilmesi
  - Kalite kontrolün sağlanması
  - Acil durumlarda ilgili kişilerle iletişim sağlanması
  - Sistem odaları, yazılımlar ve kullanılan uygulamalar kapsamında veri güvenliğinin sağlanması
- Şirket içerisinde güvenliğin sağlanması özellikle işyeri güvenliğinin sağlanması amacıyla,
- Finans ve muhasebe işlerinin yürütülmesi,
- Görevlendirme süreçlerinin yürütülmesi,
- İletişim faaliyetlerinin yürütülmesi,
- İş faaliyetlerinin yürütülmesi/denetimi,

- İş sağlığı ve güvenliği faaliyetlerinin yürütülmesi(taşeron çalışanları için),
- Lojistik faaliyetlerinin yürütülmesi,
- Mal hizmet alım ve satım ile operasyon süreçlerinin yürütülmesi,
- Sözleşme süreçlerinin yürütülmesi, taşınır mal ve kaynaklarının güvenliğinin temini,
- Veri sorumlusu operasyonlarının güvenliğinin temini,
- Yetkili kişi kurum ve kuruluşlara bilgi verilmesi,
- Yönetim faaliyetlerinin yürütülmesi,
- Pazarlama ve analiz faaliyetlerinin yürütülmesi
- Fiziksel mekan güvenliğinin temini
- Reklam/Kampanya/Promosyon faaliyetlerinin yürütülmesi

b. İmhaya İlişkin Esaslar

Saklamaya ilişkin açıklamalar imha için de geçerli olmakla birlikte 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,
- Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Kurum tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4. KİŞİSEL VERİLERİN SAKLANMASI VE İMHA SÜRECİNDE YER ALAN BİRİMLAR, UNVANLARI VE GÖREV TANIMLARI

Hastanemizin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına aşağıda yer alan tabloda (Tablo 1) yer verilmiştir.

Tablo 1: *Saklama ve imha süreçleri görev dağılımı*

Personelin Unvanı	Birimi	Görev Tanımı
BİRCAN ÖNGÖR	YÖNETİM	GENEL MÜDÜR
YASEMİN TÜRKMEN	İDARİ HİZMETLER	İDARİ HİZMETLER DİREKTÖRÜ
ZİYNET KARADAĞ	KALİTE	KALİTE YÖNETİM DİREKTÖRÜ
SALİHA HANCI	SAĞLIK HİZMETLERİ	BAŞHEMŞİRE

5. KİŞİSEL VERİ KAYIT ORTAMLARI

Kişisel veriler, Hastanemiz tarafından aşağıda yer alan tabloda (Tablo 2) listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: *Veri Kayıt Ortamları*

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
• Sunucular (yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) • Yazılımlar (ofis yazılımları, portal, ….) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Yazıcı, tarayıcı, fotokopi makinesi	• Kağıt • Manuel veri kayıt sistemleri (*anket formları, ziyaretçi giriş defteri, aday formları, eşya buluntu formu/eşya teslim tutanağı, görüş ve öneri formu, iş başvuru formu, personel bilgi formu, Hastane nezdinde tutulan her türlü form)* • Yazılı, basılı, görsel ortamlar • Birim Dolapları • Arşiv

6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için

Hastanemiz tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde aşağıda belirtilen tedbir ve önlemler alınmaktadır.

1. Güvenlik

Hastanemiz Kanun'a uygun olarak kişisel verilerin hukuka aykırı biçimde erişilmesini ve işlenmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktadır.

2. Denetim

Hastanemiz yukarıda açıklanan veri güvenliğinin tesisi ve alınan tedbirlerin düzenliliğini ve devamlılığını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Bu kapsamda hem Hastane içerisinde bir ekip oluşturulmuş olup hem de dışarıdan destek alınmaktadır.

3. Gizlilik

Hastanemiz, ilgili veri sorumluları ve veri işleyenlerin, sahip oldukları kişisel verileri Kanun ve Politika hükümlerine aykırı olarak başkasına açıklamamaları ve işleme amacı dışında kullanmamaları için teknolojik imkân ve uygulama maliyetlerine göre gerekli tüm teknik ve idari tedbirleri almaktadır. Bu kapsamda Hastane çalışanlarımız ile Kanun ve Politika hakkında bilgilendirilme ve eğitim çalışmaları yapılmaktadır.

4. Kişisel Verilere Yetkisiz Erişim

Hastanemiz tarafından işlenen kişisel verilerin Kanun'a uygun olmayan yollarla başkaları tarafından elde edilmesi halinde, Hastanemiz bu durumu en kısa sürede ilgili kişine ve Kurul'a bildirilmesi için gerekli işlemleri yürütür. Kurul tarafından gerekli görülmesi halinde bu durum Kurul'un internet sitesinde ya da Kurul tarafından uygun görülecek başka bir yöntemle ilan edilebilir.

5. İlgili Kişilerin Yasal Haklarının Gözetilmesi

Hastanemiz, ilgili kişilerin Politika ve Kanun'un uygulanması ile tüm yasal haklarını gözetir ve bu haklarının korunması için gerekli tüm önlemleri alır.

6. Özel Nitelikli Kişisel Verilerin Korunması

Kanun'un 6. maddesine göre 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 verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel veriler, işlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına veya mağduriyete neden olma riski taşıyan veriler olup diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir. Bu nedenle Hastanemiz tarafından hukuka uygun olarak işlenen bu tür kişisel verilerin korunması için gerekli tüm tedbirler hassasiyetle alınır.

Bu çerçevede alınan teknik tedbirler aşağıdaki gibidir:

- Sızma (Penetrasyon) testleri ile Hastanemiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Hastanemizin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (ISO27001 standartlarında sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Hastane içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Hastanemiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik

güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

- 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 şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.
  - Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
  - Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,
  - Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
  - Gizlilik sözleşmelerinin yapılması,
  - Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
  - Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
  - Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,
  - Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise
  - Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
  - Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
  - Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
  - Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
  - Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
- Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- Özel nitelikli kişisel veriler aktarılacaksa
- Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
- Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
- Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.
- Kişisel verilerin işlenmesinde Kanunun 4 üncü maddesinde yer alan genel ilkeler başta olmak üzere, Kanunda yer alan bütün esaslara riayet edilir.
- Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Bakanlık ile bağlı ve ilgili kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla Bakanlık tarafından, bağlı ve ilgili kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemleri kurulabilir.
- Hiç kimse, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanamaz.
- Sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirler alınır.
- Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleme tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır.
- Herkes, veri sorumlusuna başvurarak kendisiyle ilgili olarak Kanunun 11 inci maddesinde yer alan hakları kullanabilir.

- Veri sorumlusuna başvuruda, Kanunun 13 üncü maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümlerine riayet edilir.
- Aydınlatma yükümlülüğünün yerine getirilmesinde, Kanunun 10 uncu maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine riayet edilir.
- ve m.6'da "Sağlık hizmeti sunumunda görevli kişiler; ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla erişebilir.
- e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanır. İlgili kişiler, gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilir. Gizlilik tercihi ve geçmiş sağlık verilerinin görüntülenememesi nedeniyle sağlık hizmeti sunumunda meydana gelebilecek aksaklık ve zararlardan Bakanlık sorumlu olmaz.
- e-Nabız hesabı bulunmayan kişilerin sağlık verilerine ise Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan istisnai amaçlarla sınırlı olmak üzere ancak;
- Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın,
- b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar,
- Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla,
- Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar,
- erişilebilir.
- Üçüncü fıkrada yer alan erişim kuralları, Bakanlığın sağlık hizmeti sunumu ihtiyaçlarına göre ve Kanunun 6 ncı maddesinin üçüncü fıkrası kapsamında Genel Müdürlük tarafından yeniden değerlendirilebilir. Böyle bir durumda aydınlatma yükümlülüğü kapsamında gereklilikler sağlanır.
- Geçmiş sağlık verilerinin herhangi bir kimse tarafından erişilmesini istemeyen kişilere ilgili gizlilik tercihi e-Nabız üzerinden sunulur. Bu gizlilik tercihini kullanan kişilerin geçmiş sağlık verilerine ancak kişinin kendisi tarafından beyan edilen telefon numarasına gönderilecek olan kodun hekim ile paylaşılması ve hekim tarafından sisteme girilmesi halinde erişilebilir.
- Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görülmesi ve bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verileri Bakanlıkça belirlenir ve sağlık personelinin bu verilere erişimine ölçülü kısıtlar getirilebilir." şeklinde belirtilen esaslara yönelik hareket edilmeli ve bu

kapsamda Şirketinizce tespit edilecek gerekli ve yeterli önlemlerin alınması sağlanmalıdır.

Hastanemiz tarafından, işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Hastanemiz tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Hastane tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Hastane içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

7. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

28.10.2017 tarihli Resmi Gazete'de Yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ***("Yönetmelik")*** 'İlkeler' başlıklı 7. Maddesi uyarınca kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi ile ilgili yapılan bütün işlemler Hastanemiz tarafından kayıt altına alınır ve söz konusu kayıtlar diğer hukuki yükümlülüklerimiz saklı kalmak kaydıyla en az 3 yıl boyunca saklanır.

Kişisel verilerin silinmesi ile bu veriler ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Buna göre veri sorumlusu olarak Hastanemiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almaktadır. Kişisel veriler aşağıda yer alan tabloda belirtilen yöntemlerle silinir.

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, veri tabanı 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.

Verilerin yok edilmesi ise, bilgilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesini ifade etmektedir. Bu kapsamda aşağıda yer alan tabloda belirtildiği şekilde yok etme işlemleri gerçekleştirilmektedir.

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makineleriyle veya yakılarak veya tamamen yırtılarak geri döndürülemeyecek şekilde yok 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.

Verilerin anonim hale getirilmesiyle, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi kastedilmektedir.

a. Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri

Hastanemiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya ilgili kişinin talebi üzerine kişisel verileri silebilir veya yok edebilir.

Hastanemiz tarafından en çok kullanılan silme veya yok etme teknikleri aşağıda sıralanmaktadır:

- **Fiziksel Olarak Yok Etme (Physical Destruction):**
  Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak silinmesi/yok edilmesi sistemi uygulanmaktadır.
- **Yazılımdan Güvenli Olarak Silme (Secure Deletion Software):**
  Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler ile dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcıların erişim haklarının kaldırılması yöntemleri kullanılır.
- **Uzman Tarafından Güvenli Olarak Silme (Sending to a Specialist for Secure Deletion)**
  Hastanemiz bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

b. Kişisel Verileri Anonim Hale Getirme Teknikleri

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Hastanemiz veri sorumlusu sıfatıyla, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almaktadır. Bu kapsamda Hastane olarak hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmekteyiz. Kanun'unun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamının dışında olup, ilgili kişinin açık rızası aranmayacaktır. Hastanemiz tarafından en çok kullanılan anonimleştirme teknikleri aşağıda sıralanmaktadır:

- **Maskeleme (Masking):**
  Kişisel verilerin belli alanlarının silinerek veya yıldızlanarak kişinin belirlenemez hale getirilmesidir. Örneğin, kişinin kredi kartı numarasının bir kısmının yıldızlanması durumunda maskeleme söz konusudur. (6698 **** **** 0006)
- **Toplulaştırma (Aggregation)/Kümülatif Data Yaratma:**
  Verilerin kümülatif hale getirilerek toplam değerlerinin yansıtılmasını ifade eder. Örneğin, Hastanede kadın çalışan sayısının Z adet olması ve sayının %40'ının üniversite mezunu, %60'ının yüksek lisans mezunu olmasına ilişkin veriler anonim hâle getirilmiştir.
- **Veri Türetme (Data Derivation):**
  Mevcuttaki detay verilerin daha genel karşılıklarıyla değiştirilmesidir. Örneğin, doğum tarihi bilgisinin Gün/Ay/Yıl detaylarının yerine kişinin direkt yaşının yazılması durumunda veri türetmek suretiyle anonimleştirme yapılmıştır.
- **Veri Karma (Data Shuffling, Permutation):**

Veri kümesi içinde değerlerin karıştırılarak toplam faydaya zarar vermeden kişilerin tespit edilebilirlik özelliğinin yok edilmesini ifade eder. Örneğin, ses kayıtlarının niteliği değiştirilerek seslerle ilgili kişinin ilişkilendirilemeyecek hale getirilmesi.

Bunlara ek olarak Hastanemiz tarafından Kurum tarafından belirtilen[1] ve aşağıda sayılan diğer anonimleştirme teknikleri kullanılabilecektir:

- Değişkenleri Çıkartma
- Kayıtları Çıkartma
- Alt ve Üst Sınır Kodlama
- Bölgesel Gizleme
- Örnekleme
- Mikro-Birleştirme
- Veri Değiş-Tokuşu
- Gürültü Ekleme
- Tekrar Örnekleme
- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA VE PERİYODİK İMHA SÜRELERİ

Hastanemiz, kişisel verileri kanunlarda ve sair mevzuatta öngörülen süreler uyarınca saklamaktadır. Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin kanunlarda ve sair mevzuatta bir süre düzenlemesi bulunmuyorsa, kişisel veriler Hastanemizin o kişisel veriyi işlediği zaman yürütülen faaliyet kapsamında kişisel veriyi işleme amacının gerçekleşmesine kadar süre boyunca işlenmekte, imha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha tarihi ve işleminde silinmekte, yok edilmekte veya anonim hale getirilmektedir. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Hastanemizce yetkilendirilen kişiler tarafından veya kurulan yazılımsal altyapı ile kendiliğinden yerine getirilir.

Hastanemiz, işleme amacı sona ermiş kişisel verileri imha etmek amacıyla 15 Ocak 15 Haziran tarihlerini periyodik imha tarihleri olarak belirlemiştir. Bu tarihlerde, işlenmesini gerektiren sebepleri ortadan kalkan kişisel veriler otomatik, yarı otomatik veya manuel olarak imha edilecektir.

Süreç bazında kişisel verileri saklama ve imha süreleri aşağıdaki gibidir:

[1] http://www.kvkk.gov.tr/yayinlar/Kisisel_Verilerin_Silinmesi_Yok_Edilmesi_veya_Ananonim_Hale_Getirilmesi.pdf s.16 vd.

Süreç	Saklama Süresi	İmha Süresi
Vekâletnameler, imza sirküleri, genel kurul kararları, aziller gibi genel Hastane kararlarına ilişkin belgeler	İlk kaydın yapıldığı tarihten itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İhale/İşyeri Açma/Bakanlıklar, Müsteşarlıklar, evrak Hazırlama Süreçleri	İhale sürecinin tamamlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hastane ortakları ve yönetim kurulu üyelerine ait bilgiler	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Üçüncü kişilerle imzalanan sözleşmeler (Kira sözleşmeleri, hizmet sözleşmeleri, organizasyon sözleşmeleri, vb.)	İlgili sözleşmenin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlara ait kişisel sağlık verileri	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanların işe alım dosyaları, özlük verileri	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği uygulamaları kapsamında elde edilen kişisel veriler	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan aday başvuru formları, özgeçmişleri	Başvuru tarihinden itibaren 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Alt yüklenici / taşeron firma çalışanlarına ait kişisel veriler	İlgili sözleşmenin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Güvenlik Kamera Görüntüleri ve Ses Kayıtları	Görüntünün ve ses kaydının alındığı tarihten itibaren 2 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Durum tespit raporu, olay tutanağı gibi güvenliğe ilişkin idari raporlar	İlk kaydın yapıldığı tarihten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İmha Kayıt/Takip Tutanakları	İlk kaydın yapıldığı tarihten itibaren 3 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hasta sağlık dosyaları	İlk kaydın yapıldığı tarihten itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hasta patoloji evrakları	İlk kaydın yapıldığı tarihten itibaren 30 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finansal / Ödeme işlemlerine ait kayıtlar	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kablosuz internet hizmet kullanımına ilişkin veriler	İlk kaydın yapıldığı tarihten itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Teknik servis ziyaretçi kayıtları	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ticari Elektronik Posta Kayıtları	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çevre ve Tehlikeli Madde Süreci Evrakları	İlk kaydın yapıldığı tarihten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Atık Yönetimi Evrakları	İlk kaydın yapıldığı tarihten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kalite Dokümanları	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde