

KİŞİSEL VERİLERİ SAKLAMA ve İMHA POLİTİKASI

1. GİRİŞ

1.1 Amaç

Kişisel Verileri Saklama ve İmha Politikası ("Politika")

Veri sorumlusu unvanı : Mehmet Haşim Gür

Veri sorumlusu adresi : Erenköy cami sokak Deniz apartmanı No.3 Daire .1 Caddebostan
Kadıköy.

Veri sorumlusu telefon : 0530 311 16 33

Veri sorumlusu e-posta : linik_hasimgur@hotmail.com

Veri sorumlusu web sitesi : http://www.hasimgur.com

veri sorumlusu tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

İşletmemiz; Hukuka uygun misyon, vizyon ve temel ilkeler doğrultusunda işlediğimiz kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

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

1.2 Kapsam

Hastalar, refakatçiler, personeller, personel adayları ve hizmet verenlere ait kişisel veriler bu Politika kapsamında olup işletmemizin yönettiği kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 Kısaltmalar ve Tanımlar

Bu Politikada yer verilen hukuki ve teknik terimlerden;

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 rızayı,

Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemini,
Çalışan	İşletme personelini,
EBYS	Elektronik Belge Yönetim Sistemini,
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 ortamları,
Hizmet Sağlayıcı	İşletmemiz ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
İlgili Kişi	Kişisel verisi işlenen gerçek kişiyi,
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 kişileri,
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kanun	24.3.2016 Tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,
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 ortamı,
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
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 envanteri,
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 işlemi,
Kurul	Kişisel Verileri Koruma Kurulunu,

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 işleme 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 işlemini,
Politika	Kişisel Verileri Saklama ve İmha Politikasını,
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
VERBİS	Veri Sorumluları Sicil Bilgi Sistemini,
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği,

İfade eder.

2. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

İşletmemiz tarafından işlenen kişisel veriler Kanun’a uygun olarak saklanır ve saklama süresi sonunda imha edilir.

2.1 Saklamaya İlişkin 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, kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

2.1.1 Kişisel Veri Saklamayı Gerektiren Hukuki Sebepler

İşlenen kişisel veriler aşağıda belirtilen hukuki sebeplerden en az birinin varlığı halinde işlenir ve saklanır.

- Kanunlarda açıkça öngörülmesi
- Sözleşmenin ifası için tarafların verilerinin işlenmesinin gerekli olması
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
- Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması
- Koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi
- Açık Rıza

2.1.2 Saklamayı Gerektiren İşleme Amaçları

1-Kimlik

Acil Durum Yönetimi Süreçlerinin Yürütülmesi

Bilgi Güvenliği Süreçlerinin Yürütülmesi

Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi

Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi

Denetim / Etik Faaliyetlerinin Yürütülmesi

Faaliyetlerin Mevzuata Uygun Yürütülmesi

Fiziksel Mekan Güvenliğinin Temini

Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi

Talep / Şikayetlerin Takibi

Diğer-ağız ve diş sağlığı alanında sağlık hizmeti

2-İletişim

Acil Durum Yönetimi Süreçlerinin Yürütülmesi

Bilgi Güvenliği Süreçlerinin Yürütülmesi

Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi

Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi

4-Özlük

Acil Durum Yönetimi Süreçlerinin Yürütülmesi

Bilgi Güvenliği Süreçlerinin Yürütülmesi

Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi

Denetim / Etik Faaliyetlerinin Yürütülmesi

Eđitim Faaliyetlerinin Yürütülmesi

Faaliyetlerin Mevzuata Uygun Yürütülmesi

Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi

Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleřtirme Süreçlerinin Yürütülmesi

Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi

Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi

Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi

6-Müşteri İşlem

Diđer-ağız ve diş sağlığı alanında sağlı hizmeti

7-Fiziksel Mekan Güvenliđi

Acil Durum Yönetimi Süreçlerinin Yürütülmesi

Denetim / Etik Faaliyetlerinin Yürütülmesi

Eđitim Faaliyetlerinin Yürütülmesi

Fiziksel Mekan Güvenliđinin Temini

İş Sağlığı / Güvenliđi Faaliyetlerinin Yürütülmesi

İş Sürekliliđinin Sağlanması Faaliyetlerinin Yürütülmesi

10-Finans

Diđer-ağız ve diş sağlığı alanında sağlık hizmeti

11-Mesleki Deneyim

Diđer-ağız ve diş sağlığı alanında sağlık hizmeti

13-Görsel Ve İşitsel Kayıtlar

Diđer-ağız ve diş sağlığı alanında sağlı hizmeti

21-Sađlık Bilgileri

Acil Durum Yönetimi Süreçlerinin Yürütülmesi

Bilgi Güvenliđi Süreçlerinin Yürütülmesi

Diđer-ağız ve diş sağlığı alanında sağlık hizmeti

2.2 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. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun işletmemiz tarafından kabul edilmesi,
- İşletmemizin, 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, işletmemiz tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

3. 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. maddesiyle Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde teknik ve idari tedbirler alınır.

3.1 Teknik Tedbirler

İşlenen kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Özel nitelikli kişisel verilere erişimi olan çalışanların periyodik olarak yetki kontrolleri gerçekleştirilmektedir.
- Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testleri düzenli olarak yapılmakta veya yaptırılmakta ve test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilere erişim yapılan yazılımların güvenlik testleri düzenli olarak yaptırılmaktadır ve test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilere uzaktan erişimlerde iki kademeli kimlik doğrulama sistemi kullanılmaktadır.
- Farklı fiziksel ortamlardaki sunucular arasında kişisel sağlık verisi aktarımı yapılacaksa sunucular arasında VPN kurularak veya sFTP yöntemleriyle aktarım yapılmaktadır.
- Dijital ortamda saklanan kişisel veriler için periyodik aralıklarla silme, yok etme veya anonim hale getirme işlemleri yapılmaktadır.

3.2 İdari Tedbirler

İşlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

Veri Güvenliği Tedbiri
Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
Anahtar yönetimi uygulanmaktadır.
Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
Çalışanlar için yetki matrisi oluşturulmuştur.
Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
Güncel anti-virüs sistemleri kullanılmaktadır.
Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dairesine teslim edilmektedir.
Kişisel veri güvenliğinin takibi yapılmaktadır.
Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

Veri Güvenliđi Tedbiri

Kişisel veri içeren ortamların güvenliđi sağlanmaktadır.

Mevcut risk ve tehditler belirlenmiştir.

Saldırı tespit ve önleme sistemleri kullanılmaktadır.

Şifreleme yapılmaktadır.

Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

Veri kaybı önleme yazılımları kullanılmaktadır.

- Çalışanlar için veri güvenliđi hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliđi konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim, bilgi güvenliđi, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler veri güvenliđi hükümleri içermektedir.
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliđi politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliđi sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliđinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliđi sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliđi sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Özel nitelikli kişisel veri güvenliđine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel verilere erişim yetkisine sahip kullanıcıların, yetki kapsamı ve süreleri net olarak tanımlanmaktadır.
- Görev deđişikliği olan ya da işten ayrılan çalışanların kendisine tahsis edilmiş envanter iade alınmaktadır.
- Kişisel veri envanteri hazırlanmıştır.

- Periyodik aralıklarla silme, yok etme veya anonim hale getirme işlemleri yapılmaktadır.

4. SAKLAMA VE İMHA SÜRELERİ

İşletmemiz tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak; saklama süreleri Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için saklama süresinin bitimini takip eden ilk periyodik imha süresinde re'sen silme, yok etme veya anonim hale getirme işlemi yerine getirilir.

4.1 Saklama Süreleri Tablosu

İŞLENEN VERİ	İLGİLİ KATEGORİSİ	KİŞİ	SAKLAMA SÜRESİ
Kimlik Bilgileri	Çalışan		Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı		İş başvurusu olumsuz sonuçlanması halinde saklanmaz
	Hasta		Tedavi bitimi itibariyle 20 yıl
	Refakatçi		Hizmet süresince
	Dışardan Hizmet Veren Gerçek Kişiler		Hizmet bitiminden itibaren 10 yıl
İletişim Bilgileri	Çalışan		Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı		İş başvurusu olumsuz sonuçlanması halinde saklanmaz
	Hasta		Tedavi bitimi itibariyle 20 yıl
	Refakatçi		Hizmet süresince
	Dışardan Hizmet Veren Gerçek Kişiler		Hizmet bitiminden itibaren 10 yıl

Kişisel Sağlık Verisi	Çalışan	Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı	İş başvurusu olumsuz sonuçlanması halinde saklanmaz
	Hasta	Tedavi bitimi itibarıyla 20 yıl
Ceza Mahkûmiyeti ve Güvenlik Tedbirleri Bilgileri	Çalışan	Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı	İş başvurusu olumsuz sonuçlanması halinde saklanmaz
Özlük	Çalışan	Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı	İş başvurusu olumsuz sonuçlanması halinde saklanmaz
Hukuki İşlem	Çalışan ve Hasta	Hukuki sürecin sonlanmasından itibaren 10 yıl
İşlem Güvenliği	Çalışan ve Hasta	2 yıl
Müşteri İşlem	Hasta	20 yıl
	Dışardan Hizmet Veren Gerçek Kişiler	Hizmet bitiminden itibaren 10 yıl
Finans	Hasta	20 yıl
	Çalışan	10 yıl
Kamera Kayıtları	Bütün Kişi Grupları İçin	15 gün
Mesleki Deneyim	Çalışan	Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Çalışan Adayı	İş başvuru süreci olumsuzsa saklanmaz
Görsel ve İşitsel Kayıtlar	Çalışan	Aktif istihdam ilişkisi sonlandıktan sonra 10 yıl
	Hasta	Tedavi bitimi itibarıyla 20 yıl

	Çalışan Adayı	İş başvuru süreci olumsuzsa saklanmaz
--	---------------	---------------------------------------

4.2 İmha Süreleri

İşletmemiz, Kanun ve Yönetmelik hükümlerince kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, işbu Politikada belirlenen esas ve usullere uygun olarak kişisel verileri resen siler, yok eder veya anonim hale getirir.

Veri sorumlusu, Kanununun 13. maddesinde belirtilen kişisel verilerin silinmesini talep etme hakkını kullanarak tarafımıza usulüne uygun şekilde başvurması durumunda;

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Talebe konu kişisel veriler, talebin alındığı günden itibaren 30 (otuz) gün içinde uygun imha yöntemi ile silinir, yok edilir veya anonim hale getirilir.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Kanununun 13. maddesinin üçüncü fıkrası uyarınca talep gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

5. PERİYODİK İMHA SÜRELERİ

Yönetmeliğin 11. maddesi gereğince, periyodik imha süresi 6 ay olarak belirlenmiştir. Buna göre, her yıl ve tarihlerinde periyodik imha işlemi gerçekleştirilir. Çalışan 10 yıl hasta 20 yıl.

6. İMHA YÖNTEMLERİ

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

6.1 Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda verilen 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.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler aşağıda verilen yöntemlerle yok edilir.

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.
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 değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.
Dijital Ortamda Yer Alan Kişisel Veriler	Dijital ortamda yer alan kişisel verilerden saklama süresi sona erenler tüm log ve arka plan işlem kayıtları ve yedekleri ile birlikte geri döndürülemez bir şekilde imha edilir.

6.3 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.

İşletmemiz kişisel verileri anonim hale getirirken yukarıda belirtilen standartlara uygun şekilde anonim hale getirme işlemi yapmaktadır. Kişisel verilerin anonim hale getirilmesi işlemi sonrasında kişisel veriler hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale gelmektedir.

7. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNU SAĞLAMAK İÇİN ALINAN TEDBİRLER

Talep üzerine ve periyodik imha süreçlerinde resen gerçekleştirilen imha işlemleri Kanun'a, Yönetmeliğe ve işbu Politikaya uygun olarak yapılır. Bu kapsamda alınmış teknik ve idari tedbirler aşağıda ayrı ayrı gösterilmiştir.

7.1 Teknik Tedbirler

- Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkileri kontrol altında tutulur.
- Kişisel verilerin yok edilmesi işlemi, verilerin geri dönüştürülemez ve denetim izi bırakmayacak şekilde yapılmasının sağlanır.

7.2 İdari Tedbirler

- Personele Kişisel verilerin korunması mevzuatı, veri güvenliği ve imha konusunda eğitim verilir.
- Yapılan imha süreçleri düzenli aralıklarla denetlenir. Tespit edilen güvenlik açıklarının giderilmesi için gereken önlemler alınır.

8. KAYIT ORTAMLARI

Kişisel veriler, kanun, yönetmelik ve ilgili diğer mevzuat hükümlerine uygun olacak şekilde saklanmaktadır. Bu kapsamda saklanan kişisel verilerin kayıt ortamları aşağıdaki tabloda gösterilmiştir.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
---------------------	-----------------------------

Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar (Meddata Yazılımı, ofis yazılımları, portal.) ✓ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ✓ Bilgisayarlar (Masaüstü, dizüstü) ✓ Mobil cihazlar (telefon, tablet vb.) ✓ Optik diskler (CD, DVD vb.) ✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi, Tıbbi cihazlar	✓ Kağıt ✓ Manuel veri kayıt sistemleri ✓ Yazılı, basılı ve görsel ortamlar
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------

9. KİŞİSEL VERİ GÜVENLİĞİ İÇİN ALINAN 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. maddesiyle Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde teknik ve idari tedbirler alınır.

9.1 Teknik Tedbirler

İşlenen kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

Veri Güvenliği Tedbiri

Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

Anahtar yönetimi uygulanmaktadır.

Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

Çalışanlar için yetki matrisi oluşturulmuştur.

Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

Veri Güvenliđi Tedbiri

Güncel anti-virüs sistemleri kullanılmaktadır.

Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik drecel

Kişisel veri güvenliđinin takibi yapılmaktadır.

Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

Kişisel veri içeren ortamların güvenliđi sağlanmaktadır.

Mevcut risk ve tehditler belirlenmiştir.

Saldırı tespit ve önleme sistemleri kullanılmaktadır.

Şifreleme yapılmaktadır.

Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

Veri kaybı önleme yazılımları kullanılmaktadır.

9.2 İdari Tedbirler

İşlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanlar için veri güvenliđi hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliđi konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim, bilgi güvenliđi, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.

- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

10. PERSONEL UNVAN, BİRİM VE GÖREV DAĞILIMI

Tüm birimler ve çalışanlar, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim 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 birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları ve görev tanımlarına ait dağılım aşağıda tablo halinde verilmiştir.

GÖREVLİ	GÖREV TANIMI
Muayenehane Sahibi Hekim	İşlenen Kişisel veri saklama ve imha süreçlerinin işbu politikaya uygun şekilde yapılmasını temin etmek, birimler arası koordinasyonu sağlamak, gerekli denetimleri yapmak, politikanın geliştirilmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Sekreter/Asistan	Çalışanların politikaya uygun hareket etmesini sağlamak, gerekli denetimleri yapmak ve muayenehane sahibi hekim tarafından verilen diğer görevleri yerine getirmek. Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

11. POLİTİKADA YAPILAN GÜNCELLEMELER

Mevzuatın değişmesi sebebiyle, Kurul kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapılabilir. Bu kapsamda yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar aşağıda düzenlenen güncellemeler tablosuna eklenir.

Güncellemeler Tablosu

18.03. 2022	Kişisel Veri İşleme ve İmha Politikası yürürlüğe girmiştir.
-------------	-------------------------------------------------------------

12. SON HÜKÜMLER

İşbu Kişisel Veri Saklama ve İmha Politikası, veri sorumlusu tarafından hazırlanarak;

- işletme içinde uygun yerlerde

Yukarıda belirtilen web sitemizden <http://www.hasimgur.com>

- ilan edilerek ilgili kişilere duyurulmuştur.