KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI

İÇİNDEKİLER

GİRİŞ

1. AMAÇ
2. KAPSAM
3. TANIMLAR
4. KİŞİSEL VERİLERİN GÜVENLİĞİNİN VE GİZLİLİĞİNİN SAĞLANMASI
4.1. KİŞİSEL VERİLERİN HUKUKA UYGUN İŞLENMESİNİ, GÜVENLİ BİR ŞEKİLDE SAKLANMASINI SAĞLAMAK, HUKUKA AYKIRI ERİŞİMİ ENGELLEMEK VE HUKUKA UYGUN İMHASINI SAĞLAMAK İÇİN ALINAN TEKNİK VE İDARİ TEDBİRLER
4.2. KİŞİSEL VERİLERİN KANUNİ OLMAYAN YOLLARLA İFŞASI DURUMUNDA ALINACAK TEDBİRLER
5. KİŞİSEL VERİLERİN SAKLANMASINI GEREKTİREN İŞLEME AMAÇLARI, KİŞİSEL VERİLERİN SAKLANMASINI GEREKTİREN HUKUKİ SEBEPLER VE KİŞİSEL VERİLERİ SAKLAMA SÜRELERİ
5.1. KİŞİSEL VERİLERİN KORUNMASINI, İŞLENMESİNİ VE SAKLANMASINI GEREKTİREN AMAÇLAR
5.2. KİŞİSEL VERİLERİN SAKLANMASINI GEREKTİREN HUKUKİ SEBEPLER
5.3. KİŞİSEL VERİLERİ SAKLAMA SÜRELERİ
6. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ
6.1. KİŞİSEL VERİLERİN SİLİNMESİNİ, YOK EDİLMESİNİ VE ANONİM HALE GETİRİLMESİNİ GEREKTİREN SEBEPLER
6.2. KİŞİSEL VERİLERİN SİLİNMESİ SÜRECİ
6.3. KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ
6.4. KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ
6.5. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ YÖNTEMLERİ
7. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ
7.1. PERİYODİK İMHA SÜRESİ
7.2. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLAR
7.3. KİŞİSEL VERİLERİN KAYIT ORTAMI
8. İŞYERİ İÇERİSİNDE KAMERA İLE İZLEME
8.1. İŞYERİNİ ZİYARET EDEN MÜŞTERİ GİRİŞ-ÇIKIŞLARI
9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI
10. POLİTİKA'NIN GÜNCELLENME PERİYODU
11. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Giriş

Türkiye Cumhuriyeti Anayasası'nın 20. maddesi uyarınca, herkes kendisi ile ilgili kişisel verilerin korunmasını talep etme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.

6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ile kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar düzenlenmiştir. Bu doğrultuda hazırlanan işbu Politika'nın amacı KVKK ve sair düzenlemeler doğrultusunda kişisel verilerin saklanmasına ve imhasına ilişkin usul ve esasların belirlenmesidir.

1. Amaç

İşbu Politika, **Fizmer Lazer Estetik Fizik Tedavi Ve Özel Sağlık Hizmetleri Ticaret Limited Şirketi ("Şirket","Şirketimiz", "Veri Sorumlusu")** tarafından gerçekleştirilmekte olan kişisel verileri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirketimiz, çalışanlarına, çalışan adaylarına, hasta(müşteri) ve yakınlarına, ortaklarına, tedarikçilerine ve bunlarla sınırlı olmamak üzere verisini işlediği her kişiye ait kişisel verilerinin, T.C. Anayasası, uluslararası sözleşmeler, KVKK ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarının etkin bir şekilde kullanmasının sağlanmasını "öncelik" olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan Politika'ya uygun olarak gerçekleştirilir.

2. Kapsam

İşbu Politika'nın kapsamı dahilinde kişisel verileri işlenen veri sahipleri aşağıdaki şekilde kategorize edilmiştir:

Çalışanlar	Şirket'e bağımlı olarak, belirli veya belirsiz süreli olarak iş gören tüm gerçek kişiler
Çalışan Adayları	Şirket'e iş başvurusunda bulunarak veya herhangi bir yolla özgeçmişini ve ilgili bilgilerini Şirket'e erişilebilir kılan gerçek kişiler
Şirket Ortakları	Şirketimizin hissedarları
Müşteriler(Hastalar)/Müşteri Adayları	Şirketimiz tarafından sunulan ürün veya hizmetlerden faydalanan kişiler veya potansiyel olarak faydalanacak kişiler
Ziyaretçiler	İşletmemize çeşitli amaçlarla girmiş olan gerçek kişiler
Tedarikçiler/Tedarikçi Adayları	Şirketimiz tarafından sunulan ürün ve hizmetlerin gerçekleştirebilmesi için şirketimize ürün, ham madde sağlayan üreticiler
Veliler	Velayet altındaki küçüğü temsil eden velayet sahibi kişi veya kişiler
Vasiler	Ana veya babanın velayeti altında olmayan küçükler ile kısıtlı ergin kimselerin kişiliği ve malvarlığı ile ilgili tüm menfaatlerini korumak ve hukuki işlemlerinde onu temsil etmekle yükümlü kanuni temsilciler
Temsilciler	Hak ve görev bakımından birinin adına davranan mümessiller

3. Tanımlar

İşbu Politika'da kullanılan tanımlar aşağıda yer almaktadır:

Açık rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Başkanlık	Kişisel Verileri Koruma Kurumu Başkanlığı'nı
Elektronik ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
Kişisel Verilerin Anonim hale getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle

	getirilmesi
Çalışan	Şirket'e bağımlı olarak, belirli veya belirsiz süreli olarak iş gören tüm gerçek kişiler
Çalışan adayı	Şirket'e iş başvurusunda bulunarak veya herhangi bir yolla özgeçmişini ve ilgili bilgilerini Şirket'e erişilebilir kılan gerçek kişiler
Tedarikçi	Şirketimiz tarafından sunulan ürün ve hizmetlerin gerçekleştirebilmesi için şirketimize ürün, ham madde sağlayan üreticiler
Kişisel Sağlık Verileri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel verilerin işlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel Verilerin Silinmesi	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel 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 envanter
Fizmer Lazer Estetik Fizik Tedavi Ve Özel Sağlık Hizmetleri Ticaret Limited Şirketi Kişisel Verilerin Saklanması ve İmhasına ilişkin Politika	Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat doğrultusunda Kişisel Verilerin Saklanması ve İmhasına ilişkin Şirket tarafından yerine getirilmesi gereken usul ve esasları belirleyen işbu Politika
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
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
KVK Kanunu	6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurulu	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
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
Sicil	Başkanlık tarafından tutulan Veri Sorumluları Sicili'ni
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Kişisel Veri Sahibi	KVKK'da "ilgili kişi" olarak addedilen, kişisel verisi işlenen gerçek kişi
Kişisel Veri Sahibi Başvuru Formu	Şirket bünyesinde kişisel verileri işlenen kişisel veri sahiplerinin KVKK'nın11. maddesinde açıklanan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi (Şirketimiz)
VERBİS	Veri Sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini
Ziyaretçi	Şirket'in tesislerine çeşitli amaçlarla girmiş olan gerçek kişiler

4. Kişisel Verilerin Güvenliğinin ve Gizliliğinin Sağlanması

Şirketimiz, KVKK'nın12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktadır.

4.1. Kişisel Verilerin Hukuka Uygun İşlenmesini, Güvenli Bir Şekilde Saklanmasını Sağlamak, Hukuka Aykırı Erişimi Engellemek ve Hukuka Uygun İmhasını Sağlamak İçin Alınan Teknik ve İdari Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka uygun işlenmesi, güvenli bir şekilde saklanması, hukuka aykırı erişimin engellenmesi ve hukuka uygun imhasının sağlanması için alınan teknik ve idari tedbirler aşağıda belirtilmiştir

1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
3. Anahtar yönetimi uygulanmaktadır.
4. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
5. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
6.Çalışanlar için yetki matrisi oluşturulmuştur.
7. Erişim logları düzenli olarak tutulmaktadır.
8. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
9. Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
10. Gizlilik taahhütnameleri yapılmaktadır.
11. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
12. Güncel anti-virüs sistemleri kullanılmaktadır.
13. Güvenlik duvarları kullanılmaktadır.
14. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
15. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

16. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
17. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
18. Kişisel veri güvenliğinin takibi yapılmaktadır.
19. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
20. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
21. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
22. Kişisel veriler mümkün olduğunca azaltılmaktadır.
23. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
24. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
25. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
26. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
27. Mevcut risk ve tehditler belirlenmiştir.
28. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
29. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
30. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
31. Saldırı tespit ve önleme sistemleri kullanılmaktadır.
32. Sızma testi uygulanmaktadır.
33. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
34. Şifreleme yapılmaktadır.
35. Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
36. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
37. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
38. Veri kaybı önleme yazılımları kullanılmaktadır.

4.2. Kişisel Verilerin Kanuni Olmayan Yollarla İfşası Durumunda Alınacak Tedbirler

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, Şirketimiz bu durumu en kısa sürede ilgili kişisel veri sahibine ve KVK Kurul'una bildirecektir.

5. Kişisel Verilerin Saklanmasını Gerektiren İşleme Amaçları, Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler ve Kişisel Verileri Saklama Süreleri

5.1. Kişisel Verilerin Korunmasını, İşlenmesini ve Saklanmasını Gerektiren Amaçlar

Şirketimiz nezdinde kişisel veriler aşağıda sayılan amaçlar çerçevesinde işlenmektedir:

- Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayı Başvuru Süreçlerinin Yürütülmesi
- Denetim/etik faaliyetlerinin yürütülmesi
- Eğitim faaliyetlerinin yürütülmesi
- Erişim yetkilerinin yürütülmesi
- Faaliyetlerin mevzuata uygun yürütülmesi
- Finans Ve Muhasebe İşlerinin Yürütülmesi
- Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
- Fiziksel Mekan Güvenliğinin Temini

- Görevlendirme süreçlerinin yürütülmesi
- İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İş Faaliyetlerinin Yürütülmesi / Denetimi
- İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi

5.2. Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler

Şirketimiz kişisel verilerin saklanması için ilgili mevzuatta bir süre öngörülüp öngörülmediğini tespit ederken aşağıda yer alan mevzuatı kontrol etmektedir:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6098 sayılı Türk Borçlar Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 4982 sayılı Bilgi Edinme Kanunu
- 4857 sayılı İş Kanunu
- 2828 sayılı Sosyal Hizmetler Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine ilişkin Yönetmelik
- 3359 sayılıSağlıkHizmetleri Temel Kanunu
- Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname
- Ayakta Teşhis Ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik
- Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Korunması Yönetmeliği
- Yürürlükte olan diğer ikincil düzenlemeler

5.3. Kişisel Verileri Saklama Süreleri

Şirketimiz kişisel verilerin saklanması için ilgili mevzuatta bir süre öngörülüp öngörülmediğini tespit eder. İlgili mevzuatta bir süre öngörülmüşse bu süreye riayet eder; bir sürenin öngörülmemiş olması takdirde kişisel verileri işlendikleri amaç için gerekli olan süre kadar muhafaza eder. Kişisel verilerin işlenme amacı sona ermiş ve ilgili mevzuat ve/veya Şirketimizin belirlediği saklama sürelerinin sonuna gelinmişse yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi, kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla saklanabilecektir. Şirketimiz tarafından işlenme amacı sona ermiş, ilgili mevzuat ve/veya Şirket'in belirlediği azami saklama sürelerinin sonuna gelinen ve herhangi bir başkaca saklanma amacı taşımayan kişisel veriler saklanmamaktadır.

T.C. Resmi Gazete ile yayınlanan ve 01/01/2018 tarihi ile yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ("Yönetmelik") 7. maddesi uyarınca, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

6. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi

KVK Kanunu'nun 7. maddesi uyarınca, kişisel verilerin ilgili mevzuata uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler re'sen veya kişisel veri sahibinin talebi üzerine Şirketimiz tarafından silinir, yok edilir veya anonim hale getirilir.

İşlenmesini gerektiren sebeplerin ortadan kalktığı hallerde kişisel verileri silmek, yok etmek veya anonim hale getirmek Şirketimizin yükümlülüklerindendir. Bunun için kişisel veri sahibinin başvurusu şart değildir. Bununla birlikte, kişisel veri sahibinin kişisel verilerinin yok edilmesini veya silinmesini talep etme hakkı bulunmaktadır.

Yönetmelik ile tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların belirlenmesi amaçlanmıştır. Yönetmelik çerçevesinde işbu Politika'yı hazırlamış olan Şirketimiz, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. Bu süre her halde altı ayı geçemez.

Yönetmelik kapsamında, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin olarak aşağıda sayılan **ilkeler** hakimdir:

- KVK Kanunu'nun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin Şirketimiz tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.
- Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde KVK Kanunu'nun 4 üncü maddesindeki genel ilkeler ile 12 nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, KVK Kurulu kararlarına ve işbu Politika'ya uygun hareket edilmesi zorunludur.
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.
- Şirket, kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri işbu Politika ve diğer prosedürlerinde açıklamakla yükümlüdür.
- Şirket, KVK Kurulu tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. Kişisel veri sahibinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer.

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

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

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Bu kapsamda, kişisel veriler, Şirketimiz, alıcı veya alıcı grupları tarafından geri döndürme ve 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

getirilmektedir. Şirketimiz tarafından, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbir alınmaktadır.

Yönetmelik'in 12. maddesine istinaden, kişisel veri sahibi, KVK Kanunu'nun 13 üncü maddesine istinaden Şirketimize başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirketimiz talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirketimiz, kişisel veri sahibinin talebini en geç otuz gün içinde sonuçlandırır ve kişisel veri sahibine bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirketimiz bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirketimiz tarafından KVK Kanununun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı kişisel veri sahibine en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

6.1. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesini 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, kişisel veri sahibinin açık rızasını geri alması,
- KVK Kanununun 11 inci maddesi gereği kişisel veri sahibinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun KVK Kurumu tarafından kabul edilmesi,
- KVK Kurumunun, kişisel veri sahibi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya KVK Kanununda öngörülen süre içinde cevap vermemesi hallerinde; KVK Kuruluna şikâyette bulunması ve bu talebin KVK Kurulu 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, KVK Kurumu tarafından kişisel veri sahibinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir

6.2. Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

-Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi

-Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi

-İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi

-İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması

6.3. Kişisel Verilerin Silinmesi Yöntemleri

-Hizmet olarak uygulama türü bulut çözümleri (Office 365, Salesforce, Dropbox gibi): Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri yetirme yetkisinin olmadığına dikkat edilecektir.
-Kağıt ortamında bulunan kişisel verilerin fiziksel olarak yok edilmesi: Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.
-Merkezi sunucuda yer alan ofis dosyaları: Dosya iletişim sistemindeki silme komutu ile silinecek veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılacaktır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilecektir.
-Taşınabilir medyada bulunan kişisel veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanacak ve bu ortamlara uygun yazılımlar kullanılarak silinecektir.
-Veri tabanları: Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinecektir.Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilecektir.

6.4. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel veriler yok edilirken, verilerin bulunduğu tüm kopyalar tespit edilecek ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer alan yöntemlerden bir ya da birkaçının kullanılmasıyla veriler tek tek yok edilecektir:

a)Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir:

i)Fiziksel yok etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medya da fiziksel olarak yok edilmektedir.

ii)Üzerine yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

b)Çevresel sistemler

Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

i)Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

ii)Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.) , SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa _blockerase_ komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanarak ya da yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

iii)Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir.

iv)Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir.

v)Mobil telefonlar (sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

vi)Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekmektedir.

vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme konutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

c)Kağıt ve mikrofiş ortamları

Söz konsuu ortamlardaki kişisel veriler, kalıcı ve fiziksel ortam olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortam kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünmektedir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel veriler ise bulundukları elektronik ortama göre yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

Ç) Bulut ortamı

Söz konusu sistemlerde yer alan kişisel veriler depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmekte ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılmaktadır. Bulut bilişim hizmet ilişkisi sona erdiğinde, kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilmektedir.

Yukarıdaki ortamlara ek olarak, arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

i) Ilgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin yukarıda yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanmaktadır.

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanmakta, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderimi sağlanmaktadır.

iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemler alınmaktadır.

6.5. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

a) Değer düzensizliği sağlamayan Anonim Hale Getirme Yöntemleri

i) Değişkenleri çıkartma: Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir.

ii)Kayıtları çıkartma: Bu yöntemde veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.

iii)Bölgesel gizleme: Bölgesel gizleme yönteminde amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer 'bilinmiyor' olarak değiştirilir.

iv)Genelleştirme: İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir.

v)Alt ve üst sınır kodlama: Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirilerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

vı) Global kodlama: Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir.

vıı)Örnekleme: Örnekleme yönteminde, bütün veri kümesi yerine kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır.

b) Değer düzensizliği sağlayan Anonim Hale Getirme Yöntemleri

i)Mikro birleştirme: Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

ii)Veri değiş tokuşu: Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

iii)Gürültü ekleme: Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkartmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Anonim hale getirmeyi kuvvetlendirici istatiksel yöntemler

i) K- Anonimlik: K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlardaki tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilmesiyle oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.

ii)L-Çeşitlilik: L-Çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.
iii)T-Yakınlık: Kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denilmektedir.

7. Kişisel Verileri Saklama ve İmha Süreleri

Yönetmelik'in 7.maddesi uyarınca, kişisel veriler, KVK Kanunu'un 5. ve 6. maddelerinde belirtilen şartlar kapsamında işlenmektedir. Bu işlenme şartlarının tamamının ortadan kalkması halinde ise, söz konusu kişisel veriler Şirket tarafından resen veya kişisel veri sahibinin talebi üzerine imha (silinme, yok edilme veya anonim hale getirilme) edilmektedir.

Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak**;**

- Tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanteri'nde
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta ve işbu Politika'da yer alır.

Aşağıdaki tabloda kişisel veri kategorisine göre, **azami** saklanma ve imha süreleri gösterilmiştir.

Kişisel Veri Kategorisi	**Saklama Süresi**	**İmha Süresi**
Kimlik Verisi	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
İletişim Verisi	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Özlük Verisi	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Müşteri İşlem Verisi	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Fiziksel Mekan Güvenliği Verisi	**2 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
İşlem Güvenliği Verisi	**2 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Mesleki deneyim verisi	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Görsel ve işitsel kayıtlar verisi	**2 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**
Sağlık verileri	**10 yıl**	**Saklama süresinin bitimini takip eden 6 ay içinde**

7.1. Periyodik İmha Süresi

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11. Maddesi uyarınca Şirketimiz, periyodik imha süresini 6 ay olarak belirlemiştir.

7.2. Kişisel Verileri Saklama ve İmha Süreçlerinde Yer Alanlar

Şirketimizin tüm birim 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.

Yönetmelik kapsamında, kişisel verilerin saklanması ve imhası işlemlerinde görev alan kişi/kişilerin bilgileri aşağıdaki tabloda yer almaktadır.

Kişisel verilerin saklama ve imha süreçlerinde yer alan kişi	**Kişinin Unvanı**	**Kişinin Çalıştığı Birim**	**Kişinin Görev Tanımı**
DR. BANU ÖNCEL	ŞİRKET MÜDÜRÜ/ SORUMLU DOKTOR	YÖNETİM	ŞİRKET YÖNETİMİNDEKİ SORUMLU DOKTOR

7.3. Kişisel Verilerin Kayıt Ortamı

Şirketimiz tarafından, Kişisel Veri Sahibi'nin kişisel verileri, evrak, dosya, CD, disket, hard disk, Şirket server, Mikro ERP, Şirket CRM (LIAS, PIN, SAM3, BAAN, KODEG) uygulamaları gibi veri saklamaya elverişli materyaller ve ortamlar ile kayıt altına alınmaktadır. Aşağıdaki tabloda hangi tür kişisel verilerin nasıl/nerede kayıt altına alındığı görülmektedir.

Kişisel Veri kategorisi	Kayıt Ortamı
Kimlik Verisi	**FİZİKEN VE DİJİTAL (SERVER)**
İletişim Verisi	**FİZİKEN VE DİJİTAL (SERVER)**
Özlük Verisi	**FİZİKEN**
Müşteri İşlem Verisi	**DİJİTAL**
Fiziksel Mekan Güvenliği Verisi	**FİZİKEN VE DİJİTAL (SERVER)**
İşlem Güvenliği Verisi	**DİJİTAL**
Mesleki Deneyim Verisi	**FİZİKEN**
Görsel ve İşitsel Kayıtlar Verisi	**FİZİKEN VE DİJİTAL (SERVER)**
Sağlık Bilgileri Verisi	**FİZİKEN**

8. İşyeri İçerisinde Kamera ile İzleme

İşyerinin ve çalışanların güvenliğini sağlama, acil durum yönetimi süreçlerinin yürütülmesi, fiziksel mekan güvenliğinin temini, iş sağlığı/güvenliği faaliyetlerinin yürütülmesi, ziyaretçi kayıtlarının oluşturulması amacıyla işyerimiz içerisinde kamera ile izleme gerçekleştirilmektedir.

KVK Kanunu'nda yer alan düzenlemeler doğrultusunda, Şirket'imiz tarafından kamera ile izleme faaliyetine ilişkin olarak internet sitemizde Aydınlatma Metninde bilgilendirme bulunmakta ve izlemenin yapıldığı alanların girişlerine izleme yapıldığına ilişkin bildirim yazısı asılmaktadır.

Kişinin mahremiyetine müdahale sonucu doğurabilecek alanlarda izleme söz konusu olmamaktadır. Güvenlik kamerası kayıtlarına yalnızca sınırlı sayıda Şirket çalışanımız erişebilmektedir. Kayıtlara erişimi olan söz konusu kişiler imzaladıkları gizlilik taahhütnamesi ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

8.1. Şirketi Ziyaret Edenlerin Giriş – Çıkışları

İşyerinin ve çalışanlarının güvenliğini sağlama, acil durum yönetimi süreçlerinin yürütülmesi, fiziksel mekan güvenliğinin temini, iş sağlığı/güvenliği faaliyetlerinin yürütülmesi, ziyaretçi kayıtlarının oluşturulması amaçlarıyla Şirket'imizi ziyaret edenlerin kişisel verilerini işleme faaliyeti gerçekleştirilmektedir.

9. Politika'nın Yayınlanması ve Saklanması

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır. Şirket'in internet sitesinden https://fizmer.com/ve işyeri içerisinde ortak kullanım alanlarından Politika'nın en güncel haline ulaşılmaktadır.

10. Politika'nın Güncellenme Periyodu

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

11. Politika’nın Yürürlüğü ve Yürürlükten Kaldırılması

Politika, Şirketimizin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika’nın ıslak imzalı eski nüshaları iptal edilerek imzalanır ve en az 5 yıl süre ile Şirketimiz tarafından saklanır.