6698 sayılı Kişisel Verilerin Korunması Kanunu Uyarınca

KİŞİSEL VERİLERİ SAKLAMA ve İMHA POLİTİKASI

IŞIK AĞIZ VE DİŞ SAĞLIĞI HİZMETLERİ LTD. ŞTİ.

İçindekiler

1. GİRİŞ

1.1. Amaç ve Kapsam

İşbu Kişisel Verileri Saklama ve İmha Politikası ("Politika"), Işık Ağız ve Diş Sağlığı Hizmetleri Ltd. Şti. ("Şirket") olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat uyarınca saklanması, silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin Şirket tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

1.2. Kapsam

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve herhangi bir nedenle Şirket nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

1.3. Kısaltmalar ve Tanımlar

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: Şirket 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: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

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.

İrtibat Kişisi: Veri sorumlusu ile ilgili kişi veya Kişisel Verileri Koruma Kurumu arasındaki iletişimin sağlanmasından sorumlu kişidir.

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

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

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 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 işlemi.
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: Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen 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 kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu tarafından oluşturulan ve yönetilen bilişim sistemi.
Yönetmelik: 8.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirket tarafından belirlenen irtibat kişisi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Verileri Saklama ve İmha Politikasına uygun olarak işlenmesi, saklanması ve imha edilmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir. Bu bağlamda görev tanımı aşağıdaki gibidir.
Tablo 1: Saklama ve imha süreçleri görev dağılımı

Unvan	Görev Tanımı
İrtibat Kişisi	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Verileri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek, ilgili kişilerin başvurularının incelenmesi ve değerlendirilmesi, saklama ve imha süreçlerinin yürütülmesi ve denetiminin yapılması ve tüm iş ve işlemlerin gerektiğinde Şirket yönetimine raporlanmasından sorumludur. Görev tanımının uygulanmasında Görev Tanımı dokümanı dikkate alınır.

Ayrıca İrtibat Kişisi, alınmakta olan teknik ve idari tedbirlerin Şirket çalışanları tarafından gereği gibi uygulanması, bölüm 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 aktif rol üstlenir.

3. KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar
Sunucular (Etki Alanı, Yedekleme, E-Posta, Veri Tabanı, Web, Dosya Paylaşım, vb.)
Yazılımlar (Ofis Yazılımları, Portal vb.)
Bilgi Güvenliği Cihazları (Güvenlik Duvarı, Saldırı Tespit ve Engelleme, Günlük Kayıt Dosyası, Anti-Virüs vb.)
Kişisel Bilgisayarlar (Masaüstü, Dizüstü)
Mobil Cihazlar (Telefon, Tablet vb.)
Optik Diskler (Cd, Dvd vb.)
Çıkartılabilir Bellekler (Usb, Hafıza Kartı, Hard Disk vb.)
Yazıcı, Tarayıcı, Fotokopi Makinesi
Elektronik Olmayan Ortamlar
Kâğıt
Manuel Veri Kayıt Sistemleri (İş Formları vb.)
Yazılı, Basılı, Görsel Ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, müşteriler, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunanlar gibi üçüncü kişilerin, şirket ve kuruluşların çalışanlarına ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir.

4.1. Saklamaya ve İmhaya İlişkin Genel İlkeler

Şirket tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilmektedir.

- Kişisel verilerin saklanması, silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'a ve ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.
- Kişisel verilerin saklanması, silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanmaktadır.
- Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Şirket tarafından seçilmektedir. Ancak, İlgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.
- Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından resen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından Şirketimize başvurulması halinde başvuru yanıtlama süreci işletilir. Bu doğrultuda;
  - İletilen talepler en geç 30 (otuz) gün içerisinde cevaplandırılmaktadır.
  - Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.

4.2. Saklamayı Gerektiren Hukuki Sebepler

İlgili kişilere ait kişisel veriler, Şirket tarafından özellikle (i) Şirket faaliyetlerinin sürdürülebilmesi, (ii) hukuki yükümlülüklerin yerine getirilebilmesi, (iii) çalışan haklarının ve yan haklarının planlanması ve ifası için Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aşağıdaki gibidir:

- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,

Şirket bünyesinde tutulan kişisel veriler, Kanun ve Şirket Kişisel Verilerin İşlenmesi ve Korunması Politikası (İlgili politikaya web sitesinden ulaşılabilir.) uyarınca, burada belirtilen amaç ve nedenlerle ilgili mevzuatta öngörülen süre kadar saklanmaktadır.

4.3. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Taraflar arasında sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin sona ermesi veya feshi akabinde ilgili mevzuatta belirlenen asgari saklama süresinin dolması,
- Veri işlemenin hukuka ve dürüstlük kuralına aykırı olması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması 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, Şirket tarafından re'sen yahut ilgili kişinin talebi üzerine, açık rızanın geri alınması halinde ilgili kişinin talebinin kabulü tarihinden itibaren silinir, yok edilir veya anonim hale getirilir.

4.4. Saklama ve İmha Süreleri

Şirket tarafından Kanun ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerin saklama ve imha sürelerinin tespitinde aşağıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır.

- Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Anılan sürenin sona ermesi akabinde veri hakkında aşağıdaki madde kapsamında işlem yapılır.
- Söz konusu kişisel verinin saklanmasına ilişkin olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;
  - Kişisel veriler, Kanun'un 6. maddesinde yer alan tanımlama baz alınarak, kişisel veriler ve özel nitelikli kişisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte

olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının Şirket nezdindeki önem derecesine göre belirlenir.

- Verinin saklanmasının Kanun'un 4. maddesinde belirtilen ilkelere uygunluğu örneğin; verinin saklanmasında Şirketin meşru bir amacının olup olmadığı sorgulanır. Saklanmasının Kanun'un 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
- Verinin saklanmasının Kanun'un 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.

Şirket tarafından tespit edilen saklama ve imha süreleri aşağıdaki tabloda yer almaktadır.

Tablo 3: Saklama ve imha süreleri

Süreç	Saklama Süresi	İmha Süresi
İş Kanunu kapsamında saklanılan veriler	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Türk Ticaret Kanunu kapsamında saklanılan veriler	İlgili evrak tarihinin bir sonraki yılından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
SGK mevzuatı kapsamında tutulan veriler	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş kazası/meslek hastalığına ilişkin bir talepte/davada kullanılabilecek dokümanlar	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması	Dava zaman aşımı müddetince	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Şirketin ilgili kişisel veriyi kullanma amacı sona ermedi ise, ilgili mevzuat gereği ilgili kişisel veri için öngörülen saklama süresi tabloda yer alan sürelerden fazla ise veya ilgili konuya ilişkin dava zamanaşımı süresi kişisel verinin tabloda yer alan sürelerden fazla saklanmasını gerektiriyorsa, yukarıdaki tabloda yer alan süreler uygulanmayabilecektir. Bu halde kullanım amacı, özel mevzuat veya dava zamanaşımı süresinden hangisi daha sonra sona eriyor ise, o süre uygulama alanı bulacaktır.

4.5. Periyodik İmha Süresi

Yönetmeliğin 11. maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket nezdinde her yıl Ocak ve Temmuz aylarının son gününe kadar periyodik imha işlemi gerçekleştirilir.

Saklama süresi dolan kişisel veriler, yukarıdaki tabloda yer alan imha süreleri çerçevesinde, belirlenen periyodlarla işbu Politikada yer verilen usullere uygun olarak silinir, yok edilir veya anonim hale getirilir. 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 3 (üç) yıl süreyle saklanır.

4.6. İlgili Kişinin Başvurusu

İlgili kişi, Şirketimize başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep edebilir. Talep edildiğinde ilgili kişinin;

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa talep yerine getirilir.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve kişisel veriler üçüncü kişilere aktarılmışsa, Şirket silinme talebiyle ilgili verinin aktarıldığı kişiyi bilgilendirir, Şirket ve bu kişi gerekli işlemleri yapar.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Şirket gerekçesini açıklayarak bu talebi reddedilebilir.

Her durumda talebin kabulü, kısmen kabulü veya ret kararlarına ilişkin cevaplar en geç otuz (30) gün içinde yazılı olarak ya da elektronik ortamda ilgili kişiye bildirilir. İlgili kişilerin başvurularının yanıtlanmasında "Başvuru Yanıtlama Prosedürü" uygulanır.

5. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINA İLİŞKİN İDARİ VE TEKNİK TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla Kanun'un 12. maddesindeki ilkeler çerçevesinde, Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır.

5.1. İdari Tedbirler

Şirket, idari tedbirler kapsamında;

- Saklanan kişisel verilere erişim, iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede ilgilisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalanır yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliği sağlanır.
- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- Kişisel verilerin bulunduğu ortama göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmasını sağlar ve bu ortamlara yetkisiz giriş çıkışları engeller.
- Kişisel verilerin işlenmesi, korunması, saklanması ve imhası bakımından Kanun tarafından alınması gerekli görülen tüm tedbirlere yer verilen gerekli süreç ve politika dokümanları oluşturulur.

5.2. Teknik Tedbirler

Şirket teknik tedbirler kapsamında;

- Kurulan sistemler kapsamında gerekli iç kontrolleri yapar.
- Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini sağlar.
- Çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.
- Kişisel verilerin yok edilmesini geri dönüştürülemeyecek şekilde sağlar.
- Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortamı, (şifreleme vb.) bilgi güvenliği gereksinimlerini sağlayacak şekilde korur.

- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerini sürekli takip ederek gerekli güvenlik testlerinin düzenli olarak yaptırılmasını sağlar.
- Özel nitelikli kişisel verilerin aktarıldığı durumlarda;
  - Verilerin e-posta ile aktarılması gerekiyor ise bunların şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmasını,
  - Verilerin taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemler ile şifrelenmesini,
  - Farklı fiziksel ortamdaki sunucular arasında aktarma gerçekleşiyor ise sunucular arasında VPN kurularak veya FTP yöntemiyle aktarmanın sağlanmasını,
  - Verilerin kâğıt ortamında aktarımı gerekiyorsa evrakın "gizlilik dereceli belgeler" formatında gönderilmesini sağlar.

6. İMHA YÖNTEMLERİ

Şirket tarafından kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıdaki tabloda yer almaktadır:

Tablo 4: Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Karartma	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. 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 görünemez hale getirilmesi şeklinde yapılır.
Bulut veya Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Yazılımdan Güvenli Olarak Silme	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

Tablo 5: Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel Yok Etme	Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel Yok Etme	Kişisel veri barındıran optik 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.
De-Manyetize Etme (Degauss)	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
Üzerine Yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Yazılımdan Güvenli Olarak Silme	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

Tablo 6: Anonimleştirme Yöntemleri

Değişkenleri Çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.
Bölgesel Gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
Genelleştirme	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.
Alt ve Üst Sınır Kodlama / Global Kodlama	Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir. Aynı kategori içinde kalan değerler birleştirilir.
Mikro Birleştirilme	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir 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. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
Veri Karma ve Bozma	Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

7. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

İşbu Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, Şirket internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Şirket nezdinde saklanır.

8. POLİTİKANIN GÜNCELLENME PERİYODU

Şirket, Kanun'da yapılan değişiklikler, Kurul kararları, sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda işbu Kişisel Verileri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar. İşbu Politikada yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

9. POLİTİKANIN ONAYLANMASI YÜRÜRLÜĞÜ GİRMESİ

İşbu Politika, Şirket kanuni temsilcisi tarafından onaylanır.

İşbu Politika, Şirket kanuni temsilcisi tarafından onaylanır. Tüm çalışanlara duyurularak yürürlüğe girer ve yürürlüğü itibarıyla tüm iş birimleri, danışmanlar, dış hizmet sağlayıcıları ve kişisel veri işleyen herkes için bağlayıcı olacaktır.

Çalışanların politikanın gereklerini yerine getirip getirmediğinin takibi, işverenin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde, aykırılığın önemli boyutta olması halinde vakit kaybetmeksizin irtibat kişisine bilgi verilecektir. Politikaya aykırı davranan çalışan hakkında, işveren tarafından yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır.