1. GİRİŞ VE POLİTİKA'NIN HAZIRLANMA AMACI VE KAPSAMI

6698 sayılı Kişisel Verilerin Korunması Kanunu, 2010 yılında kişisel verilerin korunmasının Anayasal bir hak olmasının ardından 2016 yılında yürürlüğe girmiş kişisel verilerin işlenmesi aşamasında özel hayatın gizliliği ilkesini muhafaza etmek ve temel hak ve özgürlüklerin zarar görmemesi adına geliştirilmiş bu konu hakkında usul ve esasları gösteren hukuki bir koruma aygıtıdır.

6698 sayılı Kanunun ("KVKK" ya da "Kanun") 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumlularının, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlama yükümlülüğü vardır. İşbu Kişisel Veri Saklama ve İmha Politikası, 6698 sayılı Kanun ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin M. İhsan Arslan Vakfı İktisadi İşletmesi ("Veri Sorumlusu") tarafından tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

İşbu politika Kanun'un ikincil düzenlemesi olan 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik'') uyarınca hazırlanmıştır.

2. TANIMLAR

Kanun/KVKK, resmi Gazetede yayınlanması ile 07/04/2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Kurul, Kişisel Verileri Koruma Kurulu

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi

Açık Rıza, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza

Kişisel Veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her tür bilgi

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

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

İmha,

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.

- Kişisel verilerin silinmesi, ilgili kullanıcı için verinin hiçbir şekilde kullanılamaz hale getirilmesi işlemi,

- Kişisel verilerin yok edilmesi, verinin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,

- Anonim Hale Getirme, kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

Kayıt Ortamı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu ortam

Elektronik Kayıt Ortamı, kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar

Elektronik Olmayan Kayıt Ortamı, elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar

Kişisel veri işleme envanteri, veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 veri saklama ve imha politikası, veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika

Periyodik imha, kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi

Veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

3. GENEL BİLGİLENDİRME VE TEMEL İLKELER

1. Kanun'un 5 ve 6 ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler veri sorumlusu sıfatıyla işletmemiz tarafından re'sen veya ilgili kişinin talebi üzerine silinip, yok edilmekte veya anonim hale getirilmektedir.
2. İlgili kişinin Kanun 'nun 11 nci maddesinde yazılı herhangi bir hakkını kullanmak adına tarafımıza iletmiş olduğu talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir.

3. İşletmemiz kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4 üncü maddesindeki genel ilkeler ile 12 nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket etmektedir.
4. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Mia tarafından kayıt altına alınmaktadır.
5. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını veri sorumlusu sıfatıyla seçmekteyiz. Ancak, ilgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilebilecektir.

4. KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler, tarafından aşağıda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Işletmemizde tutulan kayıt defterleri, elektronik ortamda da tutulabilir. İlgili kişilerin sağlık bilgilerine ait gerekli kayıtların elektronik ortamda saklanmasının, değiştirilmesinin ve silinmesinin önlenmesi ve gizliliğin ihlal edilmemesi için fiziki, manyetik veya elektronik müdahalelere ve olası suistimallere karşı gerekli idari ve teknik tedbirler alınır.

İşletmemiz tarafından fiziki ortamda tutulan kayıtların her türlü suistimale karşı korunmasına yönelik gerekli idari ve teknik tedbirler alınır. Bu konudaki gerekli idari ve teknik tedbirlerin alınmasından ve periyodik olarak denetlenmesinden mesul müdür sorumludur. Elektronik ortamdaki veriler, güvenli yedekleme sistemiyle düzenli olarak yedeklenir.

A. ELEKTRONİK ORTAMLAR:

1. Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)

2. Yazılımlar (Muhasebe yazılımları)

3. İşletme bilgisayarları (Masaüstü, dizüstü)

4. Optik diskler (CD, DVD vb.)

5. Çıkartılabilir bellekler (USB, hafıza kartı vb.)

6. Yazıcı, tarayıcı, fotokopi makinesi

7. Pos Makinaları

9. Ödeme Kaydedici Cihazlar.

10. Tıbbi Cihazlar (Lam, tüp, biyolojik örnek saklanan diğer materyaller vb.)

11. Kamera Kayıt Sistemleri

B.ELEKTRONİK OLMAYAN ORTAMLAR:

1. Kağıt (Formlar, Onamlar, Kayıt Dosyaları, Anketler, Tutanaklar, Özlük Dosyaları, Sonuçlar, Raporlar, Laboratuvar Cihaz Çıktıları Vb.)
2. Manuel veri kayıt sistemleri
3. Yazılı, basılı, görsel ortamlar

5.KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

İşlenen kişisel veriler ve kişisel sağlık verilerinin sınırları, işletmemiz verilen hizmetlerin türü ve niteliğine göre değişebilmektedir. Huzurevi, engelli bakım, rehabilitasyon, eğitim hizmetleri kapsamında verilecek hizmetin mahiyetine göre ilgili kişiden toplanacak veriler değişkenlik gösterir.

İlgili kişilere ait kişisel veriler, veri sorumlusu sıfatıyla işletmemiz tarafından, kanunlarda açıkça öngörülmesi, verilen hizmetin gerektirdiği ölçüde işlenmesi, sözleşme kurulması ve ifası, iş akdi, satış ve hizmet sözleşmeleri gibi karşılıklı edimlerin ifası için fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Daha açık bir ifadeyle saklamayı gerektiren hukuki amaç ve sebepler aşağıdaki gibidir:

Amaçlar;

1. Faaliyet konusu hizmetin kanunlarda öngörüldüğü şekilde verilebilmesi,
2. Ticari faaliyetlerin sürdürülebilmesi,
3. Hukuki yükümlülüklerin yerine getirilebilmesi,
4. Çalışan haklarının ve yan haklarının planlanması ve ifası,
5. Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi,
6. Yaşlı, engelli, öğrenci ilişkilerinin yönetilebilmesi,
7. İlgili kişilere ait bir hakkın tesisi, kullanılması veya korunması,
8. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaati için veri işlemenin zorunlu olması,
9. İlgili Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
10. KVKK Madde 5/2'de sayılan şartlardan birinin varlığından söz edilemeyecek durumlarda, saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

Hukuki Dayanaklar;

1. 6698 sayılı Kişisel Verilerin Korunması Kanunu,
2. 6102 sayılı Türk Ticaret Kanunu,
3. 6098 sayılı Türk Borçlar Kanunu,
4. 213 Sayılı Vergi Usul Kanunu,
5. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
6. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
7. 4857 sayılı İş Kanunu,3308 sayılı Mesleki Eğitim Kanunu,
8. 2547 sayılı Yükseköğretim Kanunu, 5434 sayılı Emekli Sandığı Kanunu,
9. 2828 sayılı Sosyal Hizmetler Kanunu,
10. Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği,
11. 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
12. Özel Huzurevleri ile Huzurevi Yaşlı Bakım Merkezleri Yönetmeliği,
13. Engelli Bireylere Yönelik Özel Bakım Merkezleri Yönetmeliği
14. Kişisel Sağlik Verileri Hakkinda Yönetmelik Sayı: 30808,
15. İnsan Doku ve Hücreleri ile Bunlarla ilgili Kalite ve Güvenliği Hakkında Yönetmelik,
16. 29.05.1979 tarihli ve 2238 sayılı Organ ve Doku Alınması, Saklanması ve Nakli Hakkında Kanun,
17. 28800 sayılı Özel Sağlik Sigortalari Yönetmeliği,
18. 23420 sayılı Hasta Hakları Yönetmeliği,
19. 28790 sayılı Tıbbi Laboratuvarlar Yönetmeliği,
20. 24046 sayılı Acil Sağlık Hizmetleri Yönetmeliği,

Yönetmelik ve kanunun çizdiği sınırlar çerçevesinde, aşağıda sayılan hallerde talep ile veya re'sen işletmemiz tarafından,

1. İlgili kişinin, Kanun'un 11 inci maddesindeki[1] haklarını kullanmak suretiyle verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabulü,

2. Veri sorumlusunun, ilgili kişinin Kanun'un 11 inci maddesindeki haklarını kullanarak başvurmasına karşın cevap vermemesi, başvuruyu reddetmesi ya da cevabın yetersiz olması sebepleriyle ilgili kişinin Kurul'a şikayette bulunması ve Kurul tarafından uygun bulunması,

3. Kişisel verinin açık rıza ile işlenmiş bulunup, ilgili kişinin bu açık rızasını geri alması,

4. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

5. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

6. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

7. Kanun'un 5. Ve 6. Maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması hallerinde SİLİNİR, YOK EDİLİR, ANONİM HALE GETİRİLİR.

6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi; hukuka uygun olarak imha edilmesi için veri sorumlusu İşletmemiz tarafından alınmış idari ve teknik tedbirler aşağıda sayılmıştır.

6.1 İŞLETMİMİZ TARAFINDAN ALINAN TEKNIK VE İDARİ TEDBİRLER

1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

2. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

---

[1] **İlgili kişinin hakları**

MADDE 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

3. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
4. Çalışanlar için yetki matrisi oluşturulmuştur.
5. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
6. Gizlilik taahhütnameleri yapılmaktadır.
7. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
8. Güncel anti-virüs sistemleri kullanılmaktadır.
9. Güvenlik duvarları kullanılmaktadır.
10. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
11. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
12. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
13. Kişisel veri güvenliğinin takibi yapılmaktadır.
14. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
15. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
16. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
17. Kişisel veriler mümkün olduğunca azaltılmaktadır.
18. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
19. Mevcut risk ve tehditler belirlenmiştir.
20. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
21. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
22. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

7. SAKLAMA VE İMHA SÜRELERİ

Veri sorumlusu işletmemiz tarafından Kanun ve ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha sürelerinin tespitinde aşağıda belirtilen ölçütlerden yararlanılmaktadır:

1. Kanun veya yönetmeliklerde, kişisel verinin saklanmasına ve imhasına ilişkin öngörülmüş olan süreye uyulmaktadır. Anılan sürenin sona ermesi akabinde veri hakkında 2 nci bent kapsamında işlem yapılır.

2. Söz konusu kişisel verinin saklanmasına ilişkin olarak kanunda veya yönetmeliklerde öngörülen sürenin sona ermesi veya ilgili söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;

- Kanun'un 6 ncı maddesine göre özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının işletmemiz açısından önem derecesine göre belirlenir.

- Verinin saklanmasının Kanun 'nun 4 üncü maddesinde belirtilen ilkelere uygunluğu sorgulanır. Saklanmasının Kanun 'nun 4 üncü maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.

- Verinin saklanmasının Kanun'nun 5 ve 6 ncı maddelerinde öngörülmüş olan istisnalardan 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.

8. KİŞİSEL VERİLERİN İMHA USULLERİ

1.Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, işletmemiz silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmiştir.

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

1.1. Kağıt Ortamında Bulunan Kişisel Veriler

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 yapılmaktadır.

1.2. İşletme Sunucularında Yer Alan Veriler

Dosyanın işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir.

1.3. Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.

1.4. Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmektedir.

2.Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

2.1. Kağıt ve Mikrofiş Ortamları

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre yerel sistemlerde belirtilen yöntemlerin bir ya da birkaçı kullanılarak yok edilmektedir.

2.2. Tıbbi Atıklar

İletmemiz içerisinde kişilerden alınan kan, sürüntü, doku örnekleri gibi biyolojik örnekleri ve işlemden sonra ortaya çıkan her türlü tıbbi patolojik atık Tibbi Atıkların Kontrolü Yönetmeliği kapsamında tedarikçi imha firmalarına aktarılır ve yok edilir.

3.Kişisel Verilerin Anonim Hale Getirme

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.

9. PERSONEL (KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASINDA YER ALAN) UNVAN, BİRİM VE GÖREV LİSTESİ

Veri Sorumlusunun tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.
Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda verilmiştir.

PERSONEL UNVAN VE BİRİMİ	SORUMLULUĞU
	VERİLERİN SAKLAMA SÜRESİNE UYGUNLUĞUNU SAĞLAMA VE PERİYODİK İMHA SÜRESİ İÇİNDE İMHA SÜRECİNİ YÖNETMEK
	VERİLERİN SAKLAMA SÜRESİNE UYGUNLUĞUNU SAĞLAMA VE PERİYODİK İMHA SÜRESİ İÇİNDE İMHA SÜRECİNİ YÖNETMEK

10. SAKLAMA VE İMHA SÜRELERİ TABLOSU

Mia tarafından, faaliyetler kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta yer almaktadır. Aşağıda ise süreçler bazında oluşturulan Saklama ve İmha Tablosu bulunmaktadır.

FAALİYET	SAKLAMA SÜRESİ	İMHA SÜRESİ
YAŞLI/ÖĞRENCİ /ENGELLİ BİREY DOSYALARI	Hukuki İlişki Süresi + 20 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
KAMERA KAYDI	3 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İNSAN KAYNAKLARI SÜREÇLERININ YÜRÜTÜLMESI	Hukuki İlişki Süresi + 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

VERGİ VE SGK İŞLEMLERİ	Hukuki İlişki Süresi + 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
ÖLÜM KAYITLARI	Ölümden itibaren 20 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
YAŞLI/ENGELLİ/ÖĞRENCİ BİLGİLENDİRİLMİŞ AÇIK RIZA SÜREÇLERİ	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
ELEKTRONİK ORTAMDA TUTULAN SAĞLIK BAKIM HİZMET SÜREÇ VERİLERİ	Süresiz	
EVRAK İMHA SÜREÇ KAYITLARI	3 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İNTERNET ERİŞİM SÜREÇLERİ	1 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
BİLGİ İŞLEM KAYIT SÜREÇLERİ	6 AY	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İSG SÜREÇLERİ	Hukuki İlişki Süresi+ 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
LOKASYON VERİLERİ	6 AY	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

11. GÜNCELLEMELER

İşbu politikada, kanun ve yönetmeliklere ve veri sorumlusu sıfatına haiz Mia'nın aldığı kararlara göre yapılan değişiklikler aşağıdaki tablodadır.

GÜNCELLEME TARİHİ	DAYANAK	DEĞİŞİKLİĞİN KAPSAMI

12.PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, veri sorumlusu tarafından her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

13. POLİTİKA'NIN YAYINLANMASI, SAKLANMASI VE GÜNCELLENMESİ:

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda saklanır ve internet sitesinde yayınlanır. İhtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

İşbu politika imza tarihinden itibaren yürürlüğe girmiş kabul edilir.

14. REFERANS DÖKÜMANLAR

-6698 Sayılı Kişisel Verilerin Korunması Kanunu

-30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik