

TEM AS ARAMA SEÇME İNSAN KAYNAKLARI HİZ. A.Ş.
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

TEM AS ARAMA SEÇME İNSAN KAYNAKLARI HİZ. A.Ş.

Adres: CADDEBOSTAN MH. HASAN ALİ YÜCEL SOK.NO:42 AY APT.KAT.2 D.11 KADIKÖY

Telefon: 0216 369 13 16

İnternet Sitesi: <http://www.temasaramasecme.com>

E-Posta: info@temasaramasecme.com

İçindekiler

1 GİRİŞ.....	2
1.1 AMAÇ.....	2
1.2 KAPSAM.....	2
1.3 KISALTMALAR VE TANIMLAR.....	2
2.SORUMLULUK VE GÖREV DAĞILIMLARI.....	4
4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR.....	5
4.1 Saklamaya İlişkin Açıklamalar.....	5
4.1.1 Saklamayı Gerektiren Hukuki Sebepler.....	5
4.1.2 Saklamayı Gerektiren İşleme Amaçları.....	6
4.2 İmhayı Gerektiren Sebepler.....	6
5.TEKNİK VE İDARİ TEDBİRLER.....	7
5.1 Teknik Tedbirler.....	7
5.2 İdari Tedbirler.....	8
6.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ.....	9
6.1 Kişisel Verilerin Silinmesi.....	9
6.2 Kişisel Verilerin Yok Edilmesi.....	10
7. SAKLAMA VE İMHA SÜRELERİ.....	10

1 GİRİŞ

1.1 AMAÇ

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), **TEM AS ARAMA SEÇME İNSAN KAYNAKLARI HİZ. A.Ş. (“TEM AS”)** gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

TEM AS ; çalışanlar, çalışan adayları, mal/hizmet sağlayıcıları, müşterileri ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, 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, TEM AS tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 KAPSAM

Veri Sorumlusu çalışanları, çalışan adayları, mal/hizmet sağlayıcıları, müşteriler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Veri Sorumlusunun işlediği kişisel verilerin tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3

KISALTMALAR

VE

TANIMLAR

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.

Çalışan:

TEM AS personeli

Çalışan Adayı:

Yeni iş imkanları bulmak amacıyla TEM AS’a başvuruda bulunan kişi

Elektronik Ortam:

Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.

Elektronik Olmayan Ortam:

Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel ve benzeri ortamlar.

Hizmet Sağlayıcı:

Kişisel Verileri Koruma Kurumu 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.
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 İşlenmesi:	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
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 gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika:	Kişisel Verileri Saklama ve İmha Politikası

Veri İşleyen:	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Kayıt Sistemi:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sorumlusu:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Yönetmelik:	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.SORUMLULUK VE GÖREV DAĞILIMLARI

Tüm TEM AS çalışanları, 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, birimleri ve görev tanımlarına ait dağılım Tablo 1’de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
İnsan Kaynakları Müdürü	İnsan Kaynakları	Çalışanların politikaya uygun Hareket etmesinden sorumludur. Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Muhasebe Müdürü	Muhasebe	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
Bilişim Uzmanı	Bilişim	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

Tablo 2: Kişisel veri saklama ortamları

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

Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS.) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) Kişisel bilgisayarlar (Masaüstü, dizüstü) Mobil cihazlar (telefon, tablet vb.) Optik diskler (CD) Çıkarılabilir bellekler (USB, Hafıza Kartı vb.) Yazıcı, tarayıcı, fotokopi makinesi, Elektronik puantaj kayıt sistemi.	Kağıt Manuel veri kayıt sistemleri (anket formları, Başvuru formları vb.) Yazılı, basılı, görsel ortamlar
--	--

4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

TEM AS tarafından; çalışanlar, çalışan adayları, mal ve hizmet sağlayıcı olarak ilişkide bulunan üçüncü kişilerin, ziyaretçi ve müşterilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 Saklamaya İlişkin Açıklamalar

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü 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.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Buna göre, TEM AS faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen ve işleme amaçlarımıza uygun süre kadar saklanır. Bu kapsamda kişisel veriler;

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,
4857 sayılı İş Kanunu,
6102 sayılı Türk Ticaret Kanunu
213 sayılı Vergi Usul Kanunu

2004 sayılı İcra İflas Kanunu

ve sair mevzuat uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

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

- Çalışan adayı ve stajyer seçme ve yerleştirme süreçlerinin yürütülmesi
- Çalışan için Sözleşmenin kurulması ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
- İnsan kaynakları süreçlerinin planlanması
- Yetkili kişi kurum ve kuruluşlara bilgi verilmesi
- İş faaliyetlerinin yürütülmesi/denetimi
- Erişim yetkilerinin yürütülmesi
- Görevlendirme süreçlerinin yürütülmesi
- Hukuk işlerinin takibi ve yürütülmesi
- İletişim faaliyetlerinin yürütülmesi
- Eğitim faaliyetlerinin yürütülmesi
- Risk yönetimi süreçlerinin yürütülmesi
- Sözleşme süreçlerinin yürütülmesi
- Acil durum yönetimi süreçlerinin yürütülmesi
- Faaliyetlerin mevzuata uygun yürütülmesi
- Finans ve muhasebe işlerinin yürütülmesi
- İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi
- Müşteri ilişkileri yönetim süreçlerinin yönetilmesi
- Yönetim faaliyetlerinin yürütülmesi
- Bilgi güvenliği sürecinin yürütülmesi
- Fiziksel mekan güvenliğinin temini
- Müşteri memnuniyetine yönelik aktivitelerin yönetilmesi ve takibi
- Çalışan adaylarının başvuru süreçlerinin yürütülmesi
- Performans değerlendirme süreçlerinin yürütülmesi
- Saklama ve arşiv faaliyetlerinin yürütülmesi
- Organizasyon ve etkinlik yönetimi

4.2 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 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,

Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyetle bulunması ve bu talebin Kurul tarafından uygun bulunması,

Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, TEM AS tarafından ilgili kişinin talebi ile veya resen silinir, yok edilir veya anonim hale getirilir.

5.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 TEM AS tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

TEM AS tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi üzerinden yapılmaktadır.

Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.

Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

5.2 İdari Tedbirler

TEM AS tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili mevzuat hakkında eğitimler verilmektedir.
- TEM AS tarafından yürütülen faaliyetlere ilişkin çalışanlara ve diğer kurumlara gizlilik sözleşmeleri imzalatılmaktadır.

- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Kurum tarafından 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 Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

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, veritabanı 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, TEM AS tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

7. SAKLAMA VE İMHA SÜRELERİ

TEM AS tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;

Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde TEM AS tarafından güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi TEM AS tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İşe Alım(Sağlık verisi içeren evraklar hariç)	Sözleşmenin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Özlük Dosyası(Sağlık verisi içeren evraklar hariç)	Sözleşmenin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Gelen Evrak(Sağlık verisi içeren evraklar hariç)	Sözleşmenin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finansal Faaliyetler	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Güvenlik Faaliyetleri	Kayıt tarihinden itibaren 30 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tüzel Kişiliğin Temsili	Temsilin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yönetim	Karar defterinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul	Karar defterinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İlan	Yayım tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuk İşlerinin Takibi(Sağlık verisi içeren evraklar hariç)	Sözleşmenin sona ermesinden ve/veya kararın kesinleşmesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Operasyonel Süreçler	Sözleşmenin sona ermesinden ve/veya işlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Veri Güvenliği Süreci	Sözleşmenin sona ermesinden ve/veya imha tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Sağlık Dosyası	Sözleşmenin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Faaliyetleri	Kayıt tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince TEM AS , periyodik imha süresini 6(altı) ay olarak belirlemiştir. Buna göre, TEM AS 'de her yıl **Şubat ve Temmuz** aylarında periyodik imha işlemi gerçekleştirilir.

9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da TEM AS şirket merkezinde bulunan dosyasında saklanır.

10.POLİTİKA'NIN GÜNCELLENME PERİYODU

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

11.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, TEM AS internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır.