AIR CLINIC İŞ GÜVENLİĞİ HİZMETLERİ LTD. ŞTİ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. POLİTİKANIN AMACI

Hazırlanan işbu Kişisel Veri Saklama ve İmha Politikası **(''Politika'')**, 6698 sayılı Kişisel Verilerin Korunması Kanunu **(''KVKK''** veya **''Kanun''**) ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik **(''Yönetmelik'')** başta olmak üzere ilgili mevzuat uyarınca Air Clinic İş Güvenliği Hizmetleri Ltd. Şti. **("Şirket")** saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul, esas, saklama, silme ve imha sürelerini belirlemek amacıyla hazırlanmıştır.

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

2. TANIMLAR VE AÇIKLAMALAR

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme/ Anonimleştirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Çalışan/Stajyer	**Şirket** çalışanları veya stajyerleri.
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.
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 anonimleştirilmesi.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yollardan işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

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.
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
KVKK, Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
Özel Nitelikli Kişisel Veri	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Kişisel Veri Saklama ve İmha Politikası
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Şirket	**Air Clinic İş Güvenliği Hizmetleri Ltd. Şti.**
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi, dizin.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi.
Yönetmelik	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

3. DÜZENLENEN KAYIT ORTAMLARI

Şirket bünyesinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklere uygun bir şekilde aşağıdaki kayıt ortamlarında hassas bir şekilde muhafaza edilir.

Elektronik ortamlar:

- Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım)
- Yazılımlar (ofis yazılımları, portal, vb.)
- MS office dosyaları
- Şirket bilgisayarları (masaüstü, dizüstü)
- Ağ cihazları
- Mobil cihazlar ve içerisindeki saklama alanları (telefon, tablet vb.)
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
- Yazıcı
- Kamera
- Tarayıcı
- Fotokopi makinesi
- Optik diskler (CD, DVD, vb.)
- Çıkartılabilir diskler (USB, hafıza kartı, vb.)
- Kolay İK

Elektronik olmayan ortamlar:

- Birim dolapları
- Birim arşivi
- Arşiv
- Kâğıt
- Yazılı, basılı, görsel ortamlar
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi defteri, aday değerlendirme formları)

4. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Şirket bünyesinde bulunan kişisel veriler Şirketin hizmetlerinin sunulması, faaliyetlerinin kesintisiz olarak sürdürülmesi, insan kaynakları süreçlerinin planlanması ve yürütülmesi, çalışan hak ve menfaatlerinin planlanması, tedarik ve iş ortağı süreçlerinin planlanması ve yürütülmesi, etkin iletişimin sağlanması, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde hukuki yükümlülüklerin yerine getirilmesi, sektöre özgü yükümlülüklerin yerine getirilmesi, gerekli kalite ve standart denetim süreçlerinin yerine getirilmesi, kamu kurum ve kuruluşlarına bilgi verilmesi, kurumsal iletişimin sağlanması, güvenliğin sağlanması,

istatistiksel çalışmaların yapılması, analiz çalışmalarının yapılması, raporlama çalışmalarının yapılması, imzalanan sözleşme ve protokollerin yüklediği edimlerin ifa edilmesi, ileride doğabilecek hukuki uyuşmazlıklarda delil olarak kullanılması veya ispat yükümlülüğünün yerine getirilmesi, yazılı, basılı ve elektronik dergi ve bülten çalışmalarının yapılması, arşiv süreçlerinin işletilmesi, tedarik zincirinin yürütülmesi amaçlarıyla aşağıda yer alan veri işleme şartları dahilinde İşbu Politikada belirtilen elektronik ya da elektronik olmayan ortamlarda güvenli ve hassas bir şekilde saklanır.

Şirket bünyesinde bulunan kişisel veriler, aşağıda yer alan veri işleme şartlarının ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine imha edilir.

- Açık rızanın varlığı,
- Kanun hükmünün varlığı,
- Fiili imkânsızlık nedeniyle açık rızanın alınamaması,
- Sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kişisel verisinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşuluyla veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması.

5. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİNİN VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.

6. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Kişisel verileri imha etmeye *(silmeye, yok etmeye ve anonim hale getirmeye)* yönelik **Şirket** bünyesinde bulunan uygulamalar aşağıdaki gibidir:

Kişisel Verilerin Silinmesi

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.
- Fiziki olarak kâğıt, dosya, klasör ortamında bulunan kişisel veriler; ilgili kullanıcıların (arşiv/saklama sorumlusu haricinde diğer tüm çalışanlar) erişemeyeceği, ulaşamayacağı ve girip inceleme yapamayacağı arşiv/saklama/depolama alanlarına ya da bu alanların ilgili bölümlerine depolanır. Burada önemli olan ilgili kullanıcıların bu muhafaza alanlarına giremeyecek ve içeride bulunan kişisel veriler üzerinde herhangi bir işlem yapamayacak olmasıdır. Saklama/depolama/arşiv alanlarının belirli bölümlerinde yine arşiv/saklama sorumluları haricinde hiç kimsenin erişemeyeceği kilitli alanlarda muhafaza edilerek silme işlemi gerçekleştirilebilir.
- Merkezi sunucuda yer alan ofis dosyaları, dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması ile gerçekleştirilmektedir.
- Taşınabilir medyada bulunan kişisel veriler (örneğin flash tabanlı saklama ortamında bulunan veriler) ise şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.
- Veri tabanlarında bulunan kişisel veriler, ilgili satırların/sütunların ya da tablo içerisinde yer alan hücrelerin veri tabanı komutları ile (DELETE vb.) silinmektedir.

Kişisel Verilerin Yok Edilmesi

- Yerel sistemler üzerindeki kişisel verilerin yok edilmesi de-manyetize etme (medyanın özel bir cihazdan geçirilerek yüksek bir değerde manyetik alana maruz bırakılması), fiziksel yok etme (Medya ve manyetik medyanın eritilmesi, yakılması, öğütücülerin kullanılması) ve üzerine yazma yöntemleriyle sağlanmaktadır.
- Çevresel sistemler üzerindeki kişisel verilerin yok edilmesi; Ağ cihazları (switch, router vb.), Flash tabanlı ortamlar/sabit disklerin (ATA “SATA, PATA vb.”, SCSI “SCSI Express vb.), Manyetik bant, Manyetik disk gibi üniteler, Mobil telefonlar (Sim kart ve sabit hafıza alanları), Veri kayıt ortamı çıkartılabilir ya da sabit olan yazıcı ve parmak izli kapı geçiş sistemi gibi çevre birimler, Optik diskler olarak belirtebileceğimiz

çevresel kayıt sistemleri dijital ortam ise ürün özelliği olarak destekleniyorsa <block erase> gibi yok etme komutunu kullanmak, dijital ortamın ürün özelliği olarak desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da "de-manyetize etme, fiziksel yok etme, üzerine yazma" olarak belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak, son olarak dijital ortam değil ise "de-manyetize etme, fiziksel yok etme, üzerine yazma" yöntemlerin uygun bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- Kağıt ve mikrofiş ortamlarında bulunan kişisel veriler bulunduğu kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan, bu verilerin bulunduğu ana ortamın yok edilerek imha işlemi gerçekleştirilmektedir.
- Bulut ortamında bulunan kişisel veriler şifrelenerek saklanmakta ve imha süresi geldiğinde yok etme komutu uygulanmaktadır.

7. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

Personel	Birim	Görev tanımı
Arşiv Sorumlusu	İnsan Kaynakları	Kişisel verilerin imha edilmesi.
Avukat	Hukuk	KVKK ile alakalı hukuki süreçlerin takip edilmesi.
Bilgisayar Mühendisi	Bilgi Teknolojileri	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması, elektronik ortamda bulunan kişisel verilerin imha süreci.
İnsan Kaynakları Personeli	İnsan Kaynakları	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
İSG Personeli	İSG	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

8. SAKLAMA VE İMHA SÜRECİ VE SÜRELERE İLİŞKİN TABLO

Şirket bünyesinde bulunan kişisel veriler; ilgili mevzuatta öngörülmesi durumunda bu mevzuatta belirtilen süre boyunca saklanmaktadır.

Kişisel verilerin işlenme amacı sona ermiş, ilgili mevzuat ve şirketin belirlediği saklama süresinin de sonuna gelinmişse, kişisel veriler olası hukuki uyuşmazlıkların çözümlenmesi,

yetkili kamu kurum ve kuruluşların hukuka uygun taleplerinin karşılanması veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi amacıyla saklanmaktadır.

Kısaltmalar:

TBK: 6098 sayılı Türk Borçlar Kanunu

TTK: 6102 sayılı Türk Ticaret Kanunu

VUK: 213 sayılı Vergi Usul Kanunu

İSG: İş Sağlığı ve Güvenliği Mevzuatı

İİK: 2004 sayılı İcra ve İflas Kanunu

TCK: 5237 sayılı Türk Ceza Kanunu

HMK: 6100 sayılı Hukuk Muhakemeleri Kanunu

İK: 4857 sayılı İş Kanunu

5651 sayılı Kanun: 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

AVK: 1136 sayılı Avukatlık Kanunu

Süreç (Faaliyet)	Faaliyetin Yasal Dayanağı	Saklamanın Yasal Dayanağı	Yok Etme Zamanı
Personel adayı değerlendirmesi	-	KVKK	Aday işe alınırsa özlük dosyasına aktarılır. Aday işe alınmazsa başvurunun olumsuz sonuçlanma tarihini takip eden ilk periyodik imha işleminde imha edilir.
Personelin özlük dosyası	İK TBK	İK TBK KVKK	Çalışanın işten ayrılmasından itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Adli sicil kayıtları	Açık rızanın varlığı araştırılır. 5352 sayılı Adli Sicil Kanunu'ndaki sürelere paralel bir şekilde güncelliği sorgulanır.		
Personelin özlük dosyası oluşturulması	İK TBK İSG	İK TBK İSG KVKK	Çalışanın işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.

Personelin kimlik bilgileri ile işe giriş ve işten çıkış bilgilerinin tutulması	İK TBK İSG	İK TBK İSG KVKK	Çalışanın işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Personel ödeme/kesinti işlemleri (İş avansı, Maaş, Prim, İkramiye, Ayni Yardımlar, Banka Promosyonları, BES, Kıdem, İhbar, İkale, İştirak, Harcırah ve Seyahat Ödemeleri gibi), Bordro	İK TBK	İK KVKK	Çalışanın işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
İşe giriş sağlık muayeneleri ve periyodik-poliklinik sağlık muayeneleri, istirahat raporları	İSG İK TBK	İSG İK TBK KVKK	Çalışanın işten ayrılma tarihinden itibaren 15 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
İş kazası tutanağı, acil durum kayıt formu, iş kazası muayenesi ve olay kayıtları, sonuç bildirimi	İSG	İSG KVKK	Çalışanın işten ayrılma tarihinden itibaren 15 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Personel izin bilgileri	İK İSG	İK İSG KVKK	Çalışanın işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
İş Sağlığı ve Güvenliği dahilinde gerçekleştirilen eğitim kayıtları	İK İSG	İK İSG KVKK	Çalışanın işten ayrılma tarihinden itibaren 15 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Denetim/Disiplin süreçleri	İK	KVKK	Çalışanın işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Zimmet süreçleri	İSG	İSG KVKK	Zimmet edilen eşyanın tesliminden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.

Araç takip sistemleri	-	KVKK	2 yıllık süre ile saklanır. Süreyi takip eden ilk periyodik imha işleminde imha edilir.
Faturalar, beyanname ve vergi süreçleri	TTK VUK	TTK VUK KVKK	Faturanın düzenlendiği/verginin tahakkuk ettiği yılın bitiminden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Beden Bilgileri	İSG	KVKK	Yıllık olarak güncellenir. 1 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Dava/icra/arabuluculuk dosyalarının tutulması	AVK HMK İİK	AVK HMK İİK KVKK	Sürecin tamamlanmasının ardından 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir. Ceza soruşturmasını gerektiren hususlarda ceza zamanaşımı süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
Ziyaretçi giriş – çıkış kayıtları	-	-	Ziyaretin gerçekleşme tarihinden itibaren 2 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Tedarikçi çalışanlarının bilgilerinin tutulması	İK TBK	KVKK İK TBK	Tedarikçi ile ilgili sözleşmesel sürecin sona erme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.

Tedarikçi bilgilerinin tutulması	TBK	KVKK TBK	Tedarikçi ile ilgili sözleşmesel sürecin sona erme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Kamera kayıtları	-	KVKK İK TBK	3 aylık süreyle üzerine yazılır
Çalışan kimlik kartı süreçleri	-	KVKK	Çalışanın işten ayrılma tarihini takip eden ilk periyodik imha işleminde imha edilir.
İhale süreçleri	TBK TTK	TBK TTK KVKK	İhale edilen işin ifasından itibaren 10 yılın sonunda imha edilir.
Kullanıcı tanımlama süreçler	-	KVKK	Çalışanın işten ayrılma tarihini takip eden ilk periyodik imha işleminde imha edilir.
Log kayıtları	KVKK İK TBK	KVKK	Kaydın alınma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Log kayıtları (5651 sayılı Kanun) / İnternet erişimi	5651 s. Kanun	KVKK 5651 s.k.	Kaydın alınmasından itibaren 2 yıllık sürenin sonunda imha edilir.
Yönetim kurulu, Genel kurul, İcra kurulu kararı	TTK	TTK KVKK	Karar tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Yönetim kurulu/üst yönetim bilgilerinin tutulması	TTK	TTK KVKK	İlgili yönetim kurulu/üst yönetim üyesinin işten ayrılma tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Tedarikçiler ile yürütülen süreç ve dokümanlar (Örn: tedarikçi ödemeleri, ödeme makbuzu, irsaliye, poliçe, mutabakat, hak ediş, icra yazıları, beyannameler, zeyilname, hizmet ve danışmanlık alımları, bildirgeler,	TBK VUK TTK	TBK VUK TTK KVKK	Tedarikçi ile sözleşmesel veya hukuki işlemin sona ermesinden itibaren 10 yılın sonunda imha edilir.

formlar, imza sirküleri, mail order)			
Sözleşme süreçleri	TBK TTK	TBK TTK	İlişkinin sona erme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
GSM giderleri/ Araç giderleri	-	TBK KVKK	Giderin yapılma tarihinden itibaren 2 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Talep, şikayet ve memnuniyet süreci (sözleşmeden kaynaklanan)	TBK	KVKK	Talep/şikayet tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Talep, şikayet ve memnuniyet süreci (sözleşmeden kaynaklanmayan)	-	KVKK	Talep/şikayet tarihinden itibaren 3 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Etkinlik/organizasyon süreçlerinde gerekli bilgilerin tutulması	-	KVKK	Etkinliğin/organizasyonun sona ermesi tarihinden itibaren 2 yıllık süreyi takip eden ilk periyodik imha işleminde imha edilir.
Acil durum planlamasının yapılması	İSG	KVKK	3 yılda bir güncellenir.
İmha tutanağı	KVKK	KVKK	Tüzel kişiliğin sona erme tarihinden itibaren 10 yıl sonra imha edilir.

9. PERİYODİK İMHA SÜRELERİ

Kişisel verilerin imha edilmesine ilişkin yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinir, yok edilir veya anonim hale getirilir. Periyodik imha, tüm kişisel veriler için **6 aylık zaman aralıklarında (Her yılın 2. ve 8. ayının sonunda) gerçekleştirilir.**

Silinen, yok edilen ve anonim hale getirilen verilere ilişkin işlemlerin bulunduğu tutanaklar diğer hukuki yükümlülükler hariç olmak üzere en az **3 yıl süre ile** saklanır.

10. MEVCUT KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASINDA YAPILAN GÜNCELLEME İÇERİĞİ TABLOSU

GÜNCELLEME TARİHİ	GÜNCELLENMEDEN ÖNCE	GÜNCELLENDİKTEN SONRA

11. TUTANAK

Yukarıda belirtilen silme, yok etme ve anonim hale getirme işlemleri; işlemleri gerçekleştiren ilgili birim müdürü, şefi ve personelinin üçlü imzası ile hazırlanan tutanak ile kayıt altına alınır.

MUHAFAZASINA GEREK BULUNMAYAN KİŞİSEL VERİLERİN İMHASINA İLİŞKİN TUTANAK

İmha Görevlisi	
İmhayı Yapan Birim	
İmhayı Yapan Birim Yetkilisi	
İmhayı Yapan Birim Personeli	
İmha Karar Tarihi – Sayısı	
Kişisel Verinin Bulunduğu Yer	
İmha Yapılan Süreç	
Nakliyeyi Yapan Firma / Kişi	
Yükleme Yapılan Araçların Plakası	
İmhanın Yapıldığı Yer	

İmhanın Yapılış Şekli	

İmha Görevlisi

İmhayı Yapan Birim Yetkilisi **İmhayı Yapan Birim Personeli**

İmha İşleminde Rol Alan Diğer Kişiler Ad, Soyad, Unvan Ve İmzaları:

Adı Soyadı	**Unvan**	**İmza**