KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

1. Amaç

İşbu politika **Ares İnovasyon Arge Yazılım Hizmetleri Ltd. Şti.'nin ("ŞİRKET")** en önemli öncelikleri arasındadır. Şirketin **A-İSG (Akıllı İş Sağlığı ve Güvenliği Yönetim Sistemi)'ye ilişkin** 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5 ve 6. maddelerinde öngörülen yükümlülüklerini yerine getirebilmesi, ayrıca temel insan hakkı olan kişisel verilerin korunması hakkına verdiğimiz yüksek önem sebebiyle, kişisel verilerin imha usul ve süreçlerini açıklamak amacıyla hazırlanmıştır.

2. Kapsam

Bu politika, Şirketimiz ile bağlantılı tüm tarafların otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla, elektronik ortamda ya da basılı dokümanlarla işlenen tüm kişisel verilerini kapsamaktadır.

3. Tanımlamalar ve Kısaltmalar

Bu doküman içinde geçen kısaltmalar ve tanımlar tabloda gösterildiği gibidir:

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Şirket	Üniversiteler Mahallesi İhsan Doğramacı Bulvarı SEM-2 Binası Bina No:27/A No:A-7 ODTÜ TEKNOKENT Çankaya/Ankara adresinde mukim Ares İnovasyon Arge Yazılım Hizmetleri Ltd. Şti.
Çerez (Cookie)	Kullanıcıların bilgisayarlarına yahut mobil cihazlarına kaydedilen ve ziyaret ettikleri web sayfalarındaki tercihleri ve diğer bilgileri depolamaya yardımcı olan küçük dosyalardır.
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 kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
İrtibat Kişisi	Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişi. (İrtibat kişisi Veri Sorumlusunu temsile yetkili değildir. Adından anlaşılacağı üzere yalnızca veri sorumlusu ile ilgili kişilerin ve Kurumun iletişimini "irtibatı" sağlamak üzere görevlendirilen kişidir.)
Kanun/KVKK	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 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 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 Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili 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 veriler ile biyometrik ve genetik veriler.
Periyodik İmha	Kişisel verilerin işlenmesi için aranan şartların 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.
Politika	Şirket tarafından oluşturulan kişisel veri koruma politikası.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği.
Kaynak:	6698 sayılı Kişisel Verilerin Korunması Kanunu- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik - Veri Sorumluları Sicili Hakkında Yönetmelik - Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ - Veri Sorumlusuna Başvuru ve Usul Esasları Hakkında Tebliğ Veri sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

Kayıt Ortamları

Kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar - A-İSG (Akıllı İş Sağlığı ve Güvenliği Yönetim Sistemi) ✓ 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, DVD vb.) ✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi	✓ Kağıt ✓ Manuel veri kayıt sistemleri (anket formları, başvuru formları, ziyaretçi giriş defteri vb.) ✓ Yazılı, basılı, görsel ortamlar

1. Uygulama

Şirket benimsemiş olduğu vizyon, misyon ve temel değerleri gereğince, idari süreçlerini ve iş süreçlerini bağlı olduğu mevzuatlar doğrultusunda yürütmek, hizmet verdiği kişilere en iyi deneyimi sağlamak için teknolojik kaynak ve altyapıları da kullanarak "veri minimizasyonu" prensibi çerçevesinde kişisel ve özel nitelikli kişisel verileri işler. Verilerin işlenmesinde kanunun 4. maddesinde belirtilen ilkeler ve 12. maddesi gereği alınması gereken tedbirler göz önünde bulundurularak işlem yapılır. Kayıt saklama ortamları, elektronik veriler için bilişim sistemi sunucuları, uygulamaları, kurumsal bilgisayarı ve depolama ortamlarıdır, basılı dokümanlar için ise ofisler ve arşivlerdir.

1.1. Saklama ve İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

İlgili kişiye ait veriler, Şirket tarafından faaliyetlerinin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının planlanması, öğrencilere ve ailelerine sunulan hizmetlerin gerçekleştirilebilmesi, iş ortakları ile süreçlerin işletilebilmesi amacıyla fiziki veyahut elektronik ortamlarda güvenli bir biçimde Kanun ve ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanır.

Saklamayı gerektiren hukuki sebepler aşağıdaki gibidir:,

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 657 sayılı Devlet Memurları 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,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik,
- Yükseköğretim Üst Kuruluşları ve Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planı
- T.C. Aile Çalışma ve Sosyal Hizmetler Bakanlığı, İş Sağlığı ve Güvenliği Genel Müdürlüğünce yayınlanan 27.02.2018 tarihli, 23240837- 010.06.02[010.06.02]-E.10255 sayılı 2018-1 Nolu Dış Genelge'si İş Sağlığı ve Güvenliği Bilgi Yönetim Sistemi (İBYS) kapsamında ve T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı, Sosyal Güvenlik Kurumu'nun 22/12/2017 tarihli İşyeri Hekimlerinde E-Reçete Uygulaması Hakkında Duyurusu'na istinaden,

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler.

Ayrıca kişisel veriler,

- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,

hukuki sebepleri ile de saklanmaktadır.

1.1.1. Saklamayı Gerektiren İşleme Amaçları

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

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Kurum güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
-
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.

- Yasal raporlamalar yapmak.
- Çağrı merkezi süreçlerini yönetmek.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

1.1.2. İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

Yönetmelik uyarınca, aşağıda sayılan hallerde kişisel veriler veya özel nitelikli kişisel veriler, Şirket tarafından re'sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- İlgili kişinin, hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi ya da kurulun gereğinin yapılması yönünde karar vermesi.

1.2. Uygulanan Teknik ve İdari Tedbirler

Şirket, bünyesinde kanunun 7'nci ve 12'nci maddesi göz önünde bulundurularak veri saklamada ve imhada teknik ve idari tedbirler alır. Alınan tedbirler aşağıda belirtildiği gibidir;

1.2.1. İdari Tedbirler

- Şirket bünyesinde bilgi güvenliği yönetim sisteminin kurulması ve işletilmesi,
- Şirket personelleri ve ilgili taraflar ile taahhütnameler ve gizlilik sözleşmelerinin imzalanması,
- İş süreçleri üzerinde risk analizlerinin gerçekleştirilmesi,
- Kişisel veri envanterlerinin oluşturulması,
- Bilgi güvenliği politika ve prosedürlerinin işletilmesi,
- Bilgi güvenliği ve kişisel veri işleme faaliyetleri hakkında eğitimlerin düzenlenmesi ve değerlendirilmesi,
- Çalışan bilgisayar vb. araç gereçlerine yetkisiz erişimlerin önüne geçmek adına söz konusu araç ve gereçleri yalnızca yetkili kişilerin kullanması,
- Şirket içi ya da bağımsız denetimler ile faaliyetlerin gözden geçirilmesi,
- Yapılan işlemler için objektif delil üretecek kayıtların oluşturulması,

1.2.2. Teknik Tedbirler

- Sızma testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- 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 ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.

- Sistemler üzerinde yazılımsal değişiklik ve/veya güncelleme yapılacağı zaman denemeler test ortamında yapılmakta, varsa güvenlik açıkları tespit edilerek gerekli tedbirler alınmakta ve yapılacak değişikliğe son hali bu işlemlerin ardından verilmektedir.
- Şirketin 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, 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 tedbirlerle ilgili teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Şirket, 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 Şirket tarafından buna uygun hazırlık çalışmaları yapılmıştır.
- 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.
- Şirket ürün sayfalarında ve uygulamalarında internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 2048 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- 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 elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır.
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.
- 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.

1.3. Veri Silme, Yok Etme ve Anonim Hale Getirme

Bu politikanın 6.1 maddesinde belirtilen şartların ortadan kalkması halinde, kişisel veriler Şirket tarafından kendiliğinden veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta ilgili kişi tarafından Şirket'e başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılır ve ilgili kişiye bilgi verilir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir,
- Durum, şartlar ve mevzuat gereği ilgili kişinin talep ettiği imha usulünün yerine başka bir imha usulünün kullanılması gerekmekteyse, durum ilgili kişiye verilecek cevapta açıklanarak, kullanılması lazım gelen usul ile imha gerçekleştirilir,
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri kendiliğinden silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilir. Ancak, ilgili kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilir.

İlgili kişinin Kanun'un 11. maddesinde gösterilen hakları kapsamında yaptığı başvurularda verilecek cevaplar ücretsiz olarak karşılanır. Her ne kadar cevabın ücretsiz verilmesi temel ilke olsa da, verilecek cevabın ayrıca bir maliyet gerektirmesi durumunda Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 7. maddesinde gösterilen ücretler Şirket tarafından ilgili kişiden talep edilebilecektir. İgili madde şöyledir:

Ücret

MADDE 7 – *(1) İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.*

(2) Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

1.3.1. Kişisel Veri Silme

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, veri tabanı 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.

1.3.2. Kişisel Veri Yok Etme

Fiziksel Ortamda Yer Alan Kişisel Veriler : Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler yakılarak veya kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde öğütülerek 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.

1.3.3. Kişisel Veri Anonimleştirme

Şirket'de anonimleştirme için verinin bulunduğu ortam ve işleme türüne göre değişken çıkarma, gürültü ekleme, mikro birleştirme yöntemlerinden biri kullanılır.

Değişken Çıkarma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden "yüksek dereceli betimleyici" olanlar çıkarılarak mevcut veri seti anonim hale getirilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilir.

Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanır.

1.4. Veri Saklama ve İmha Süreleri ve Sorumluları

1.4.1. Veri Saklama ve İmha Sorumluları

Unvan	Görev	Sorumluluk
Birim Belge Yöneticisi	Devlet Arşiv Hizmetleri Hakkında Yönetmelik md. 6 gereğince görevli personel	Biriminde veri saklama ve imha işlemlerini gerçekleştirmek,

Kurum Belge Yöneticisi	Devlet Arşiv Hizmetleri Hakkında Yönetmelik md. 6 gereğince görevli personel	Kurumda veri saklama ve imha işlemlerini gerçekleştirmek ve ilgili birimlerin veri saklama ve imha işlemlerinin gerçekleştirilmesine destek vermek,
Üst Yönetim	Şirket iş süreçlerinden sorumlu yönetici	Şirketde veri saklama ve imha işlemlerinin uygun gerçekleştirildiğinin denetlemek ya da denetlenmesini sağlamak,

1.4.2. Veri Saklama ve İmha Süreleri

Veri saklama ve imha süreleri kişisel veri envanterinde detaylı olarak gösterilir. Verilerin saklama ve imha süreleri aşağıda belirtildiği gibidir. Kişisel veriler, saklama şartlarının ortadan kalkması üzerine, ilgili kişinin talebi ile veya süresinin gelmiş olması durumunda periyodik imha süresinde Şirket'nin uygun göreceği imha usulü ile imha edilir. Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket'de her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
Şirket İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kurum İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı	Etkinliğin sona ermesini takiben ilk periyodik imha süresine kadar	Saklama süresinin bitimini takip eden takip eden ilk periyodik imha süresinde

Sorumluluk

Şirketin 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 gösterilmiştir.

Görev	**Birim**	**Unvan**
Dokümanın Hazırlanması:	KVKK Komisyonu (Tüm çalışanların katkısı ile)	KVKK Komisyon Üyeleri
Dokümanın Kontrolü:	KVKK Komisyonu	KVKK Komisyon Üyeleri
Dokümanın Güncellenmesi:	İrtibat Kişisi	Bilgi İşlem Daire Başkanı
Dokümanın Uygulanması:	Tüm çalışanlar ve veri işleyenler	Tüm çalışanlar ve veri işleyenler

Güncelleme Kayıtları

Güncelleme No	**Tarih**	**Güncelleme Nedeni**	**Güncelleme Sayfa No**	**Güncellenen Bölüm**
1	31/12/21	Yasal yükümlülük	1	Yeni Düzenleme