1.0 GİRİŞ

Kişisel Verilerin önemi özellikle son 30 yılda ortaya çıkan teknolojik gelişmeler ve dijital çağın getirileri doğrultusunda büyük bir önem arz etmeye başlamış olup, özellikle Anayasa ve Türk Ceza Kanunu'nda yapılan düzenlemelerin ardından, taslak halinde olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK ya da KVK Kanunu) Türkiye Cumhuriyeti Büyük Millet Meclisi tarafından kabul edilmiş ve 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir.

Avcı Kalıp Sac Metal Makine San.Tic.Ltd.Şti olarak KVK Kanununa ve kişisel verilerin korunmasına yönelik uyumun sağlanması amacıyla gerekli adımlar atılmış olup, KVK Kanunu kapsamında kişisel verilerin korunmasına ilişkin tedbirler uygulamaya geçirilmiş ve bu kapsamda işbu Kişisel Verilerin Saklanması ve İmhası Talimatı, Avcı Kalıp tarafından yürürlüğe konulmuştur.

2.0 AMAÇ VE KAPSAM

İşbu Kişisel Verilerin Saklanması ve İmhası Talimatının amacı; Avcı Kalıp (Şirtket) tarafından tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlenen kişisel verilerin işlenme sürelerinin belirlenmesi ve işleme süresi ve/veya işleme amacı ortadan kalkan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların belirlenmesidir.
İşbu Saklama ve İmha Talimatı'nda, 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkındaki Yönetmeliğin 6. maddesinde yer alan veri güvenliğini sağlamak için alınmış teknik ve idari tedbirlere de yer verilmektedir.
30 Aralık 2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik hükümleri ile KVK Kurulu tarafından tavsiye niteliğinde hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi de bu çerçevede dikkate alınmıştır.
İşbu Saklama ve İmha Talimatı, KVK Kanunu 7. maddesi uyarınca 'veri sorumlusu' sıfatıyla Avcı Kalıp Sac Metal Makine San.Tic.Ltd.Şti.'nin çalışan adaylarına, çalışanlarında, eski çalışanlarından, gerçek kişi iş/çözüm ortaklarından, iş/çözüm ortağı yetkilisi ve çalışanlarından, tedarikçilerinden, müşterilerinden, stajyerlerinden ve ziyaretçileriden tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlediği, elektronik ortamlarda, kağıt ortamlarda ve işbu Talimatta belirtilen diğer kayıt ortamlarında yer alan ve işleme şartları sona ermiş tüm Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini kapsamaktadır.

3.0 TANIMLAR

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza
Alıcı Grubu	Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
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
KVKK / KVK Kanunu	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 kişiyle eşleştirilebilen her türlü bilgi
Kişisel Verilerin İmhası	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olamk kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirlen her türlü işlem
Kişisel Verilerin Silinmesi	Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılmaz hale getirilmesi

Kişisel Verilerin Yok Edilmesi	Kişisel Verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi
KVKK Kurulu	Kişisel Verileri Koruma Kurulu
KVKK Kurumu	Kişisel Verileri Koruma Kurumu
Özel Nitelikli Kişisel Veri	Kişilerin ırtkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri. Talimatta aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte 'Kişisel Veriler' olarak adlandırılacaktır.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imhan talimatında belirtilen ve tekrar eden aralıklarla gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
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

İşbu Saklama ve İmha Talimatında yer almayan tanımlar için KVK Kanunu'nda belirtilen tanımlar geçerlidir.

4.0 POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI

Tamamen veya kısmen otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam kayıt ortamı olarak adlandırılmaktadır. Bu ortamlar genel olarak aşağıdaki gibidir:

• **Fiziki Ortamlar:** Kişisel verilerin kağıt üzerine basılarak tutulduğu ortamlardır.

• **Yerel Dijital Ortamlar:** Şirket bünyesinde yer alan bilgisayarlar, sunucular, sabit yada taşınabilir diskler, optik diskler gibi sair ortamlardır.

• **Bulut Ortamlar:** Şirket bünyesinde yer almamakla birlikte, Şirketin kullanımında olan kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlar.

Yukarıda sayılan ortamların yanında Şirket tarafından işlenen Kişisel Veriler aşağıda belirtilen ve ileride ortaya çıkabilecekkayıt ortamlarında da saklanabilecektir;

• Ağ Cihazları
• Mikrofiş
• Yazıcı, Parmak Okuyucu gibi çevre birimler,
• Flash Hafızalar.

5.0 KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK YA DA DİĞER SEBEPLER

Avcı Kalıp bünyesindeki çeşitli departmanlar tarafında iş tanımları doğrultusunda yürütülen iş süreçleri ve bu süreçlere bağlı faaliyetleri gerçekleştirebilmek amacıyla çalışanların, çalışan adaylarının, eski çalışanlarının, habere konu olan kişilerin, gerçek kişi iş/çözüm ortaklarının, iş/çözüm ortaklarının çalışanları ve yetkililerinin, tedarikçilerin, müşterilerin, stajyerlerinin ve ziyaretçilerinin olmak üzere farklı ilgili kişi kategorilerine ait kişisel verileri işlemektedir.
KVK Kanunu madde 5'te yer alan işlenme şartlarına uygun olarak işlenen veriler, bu hukuki sebepler ile uyumlu olarak, mevzuatta öngörülen veya ilgili departman tarafından kişisel veri işleme amacı çerçevesinde belirlenen süreler boyunca saklamaktadır.
Bu doğrultuda saklamayı gerektiren hukuki sebepler aşağıdaki gibidir;

a) Şirket faaliyetlerinin yerine getirilmesi uyarınca, İlgili Kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından İlgili Kişinin açık rızasının bulunması,
b) Kişisel Verilerin ilgili kanunlarda ve mevzuatlarda açıkça öngörülmesi,
c) Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
d) Şirket faaliyetleri uyarınca temas halinde olan İlgili Kişilerin, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunması veya rızasına hukuki geçerlik tanınmaması sebeiyle, kendisinin veya bir başkasının hayatı ve beden bütünlüğünün korunabilmesi için saklanmasının zorunlu olaması,
e) Kişisel verilerin Şirket'in yerine getirmekte olduğu faaliyetler kapsamındaki hukuki yükümlülüğünü yerine getirmesi,

f) Şirket tarafından yürütülen faaliyetler ile uyumlu olarak, İlgili Kişinin kendisi tarafından alenileştirilmesi,
g) Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
h) Kişisel verilerin kişilerin temel ha ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanması

Tüm bu akış Kişisel Veri İşleme Envanterinde yer almaktadır. İlgili saklama süreleri sona erdiğinde ise, işbu Talimatta belirlenen silme, yok etme veya anonim hale getirme yöntemleri ile işleme amacı ortadan kalkan kişisel veriler aşağıdaki sebeplerle Şirket tarafından re'sen veya talep üzerine imha edilir;

a) İlgili Kişinin açık rıza şartına bağlı olarak işlenerek saklanmakta olan Kişisel Veriler, İlgili Kişinin rızasını geri alması halinde,
b) Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değişmesi veya ortadan kaldırılması,
c) Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
d) Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
e) Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olduğunun tespit edilmesi,
f) Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
g) İlgili kişinin, KVK Kanunu madde 11/1(e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu olarak Şirket tarafından kabul edilmesi,
h) Şirket'in, İlgili Kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, Şirketin verdiği cevabın İlgili Kişi tarafından yetersiz bulunması veya Şirket'in KVK Kanunu'nda öngörülen süre içinde cevap vermemesi hallerinde, İlgili Kişinin KVK Kurulu'na şikayette bulunması ve bu talebin KVK Kurulu tarafından uygun bulunması,
i) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

6.0 KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

KVK Kanunu'nun 12. maddesinin birinki fıkrasında; Veri Sorumlusu'nun; Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek, Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek,

Kişisel Verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu düzenlenmiştir.
Veri Güvenliğinin sağlanması yükümlülüğü çerçevesinde Şirket tarafından yürütülen faaliyetler uyarınca işbu politikada belitilen sebeplerle saklanmakta olan Kişisel veriler için başlıca aşağıdaki idari ve tekink tedbirler alınmıştır.

6.1. İdari Tedbirler

• **Mevcut risk ve tehditlerin belirlenmesi:** Şirket tarafından Kişisel Veri İşleme Envanteri hazırlamak, işlenen verilerin kategorileri, işleme amacı, aktarıldığı alıcı grupları, saklama süreleri, verisi işlenen ilgili kişi durubu belilenerek kişisel verilere ilişkin süreç ortaya çıkarılarak alınması gereken tedbirler belirlenmiştir.

• **Çalışanların eğitilmesi ve farkındalık çalışmaları:** Kişisel verilerin korunmasına ilişkin kurum kültürünün oluşturulabilmesi için kişisel verinin neyi ifade ettiği, kişisel verilerin korunmasının önemi ve gizlilik konularında şirket çalışanlarına eğitimler verilmektedir.
• Temel eğitim ve farkındalık çalışmalarının yanı sıra, kişisel verilerin işlenmesine ilişkin talimatların değişmesi halinde, yeni politikalara uyum sağlamak amacıyla verilen eğitimler tekrarlanmaktadır.
• **Kişisel verilerin güvenliğine ilişkin talimatlara uyumun sağlanması:** KVK Kanunu kapsamında veri sorumlusu sıfatıyla Şirket olarak hazırlamakla yükümlü olduğumuz politikaların yanı sıra Şirket çalışanlarına yönelik olarak gizlilik talimatları revize edilmekte ve iç etik kuralları, bilgi güvenliği politikası gibi metinler kanun kapsamında revize edilerek uyulması gerekn usul ve yasaklar hakkında çalışanlar bilgilendirilmektedir.
• **Minimum veri işleme:** Veri Sorumlusu sıfatıyla Şirket'in kişisel veri işleme amaçları çerçevesinde en az sayıda veri işlemesi sağlanmakta ve işlenme ihtiyacı duyulmayan veriler de kişisel veri saklama ve imha talimatı uyarınca silinmekte, yok edilmekte ya da anonim hale getirilmektedir.
• **Veri işleyenlerle ilişkilerin yönetimi:** KVK Kanunu'nun 12/II. Maddesi uyarınca kişisel verilerin güvenliğinin sağlanması noktasında veri işleyenlerden de gerekli taahhütler alınmakta, iş ilişkisi içerisinde bulunulan iş ortaklarımız, tedarikçilerimiz, müşterilerimiz, çözüm ortaklarımız ile kişisel verilerin işlenmesine, muhafazasına ilişkin protokoller imzalanarak, Şirket tarafından KVK Kanunu madde 5'te yer alan hukuki sebeplerle işlenen ve 3. kişilere aktarılan verilerin muahfazası ve güvenliği sağlanmaktadır.
• **Kişisel verilerin işlenmesi talimatlarının yönetimi:** Saklanan kişisel verilere erişim iş tanımı gereği erişmesi gerekli personel ile sınırlandırılmaktadır. Kişisel verilerin işlenmesi, muhafazası, imhasına ilişkin süreçlerin takibi, kişisel verilere ilişkin Şirkete iletilen taleplerin yönetimi için Şirket içerisinde

görevlendirmeler yapılmaktadır. Kişisel verilere ilişkin süreçlerin KVK Kanunu'na uygun olarak yerine getirilmesi için profesyonel danışmanlık alınmaktadır.

• **Kişisel verilerin işlenmesi ve güvenliğine ilişkindenetimler:** Şirket, KVK Kanunu hükümlerinin uygulanmasını sağlamak amacıyla gerekli iç denetimleri yapmaktadır.

• **Kişisel verilerin saklanmasına ilişkin diğer idari uygulama ve tedbirler:** İşlenen Kişisel Verilerin güvenliğinin sağlanması amacıyla Şirket bünyesinde yukarıda belirtilenlere ek olarak, genel olarak aşağıdaki idari tedbirler uygulanmaktadır;

- Çalışanlar İçin Disiplin Düzenlemeleri,
- Çalışanlara Verilen Eğitim ve Farkındalık Çalışmaları
- Çalışanlar İçin Yetki Matrisleri
- Çalışanların Erişim Yetkilerinin Gerektiğinde Güncellenmesi
- Erişim, Bilgi Güvenliği, Saklama, Kullanım, İmha Talimatlarının Oluşturulması
- Gizlilik Taahhütnamelerinin Alınması
- Sözleşmelerde Veri Güvenliğine ilişkin Hükümlerin Eklenmesi
- Kişisel Veri Güvenliği, Talimat ve Prosedürlerin Belirlenmesi
- **Kişisel Veri Güvenliğine İlişkin Sorunların Takibi ve Raporlanması**
- Kişisel Verilerin Minimuma Azaltılması
- Kanun İçi Periyodik Güncellemelerin Yapılması
- Mevcut Risk ve Tehdit Kontrolleri
- Özel Nitelikli Kişisel Verilere İlişkin Talimat ve Prosedürlerin Uygulanması
- Veri İşleyen Hizmet Sağlayıcının Veri Güvenliği Konusunda Farkındalığı sağlanmaktadır.

6.2. Teknik Tedbirler

• **Siber Güvenliğin Sağlanması:** Kişisel Veri Güvenliğinin Sağlanması amacıyla siber güvenlik sistemleri kurulmuştur ve güncelliği sağlanmaktadır. Bu kapsamda;

- İnternet üzerinden gelen izinsiz erişim tehditlerine karşı alınabilecek öncelikli tedbirler olarak güvenlik duvarı ve internet ağ geçidi kullanılmaktadır.
- Kullanılmayan yazılım ve servisler kaldırılarak yazılımların eski sürümlerinin güvenlik açıkları içermesi ihtimaline karşılık bu yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir
- Özellikle kişisel verilerin yer aldığı sistemlerin yönetilmesi amacıyla dışarıdan temin edilen yazılımların ve modüllerin güncelliğinin takibinin sağlanması amacıyla yama yönetimi ve yazılım güncellemeleri gerçekleştirilerek olası güvenlik açıklarının kapatılması sağlanmaktadır.

• **Yetki matris ve kontrolü:** Kişisel veri içeren sistemlere erişim sağlayacak personelin görev tanımıyla uyumlu olarak sınırlandırılmıştır.

- Özellikle Şirket çalışanlarının elektronik ve fiziki ortamlarda kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlamaktadır.
- Kaba kuvvet algoritması kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişkileri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle de erişim sınırlandırılmaktadır.
- Yetki matris ve kontrol sistemi kapsamında kullanıcıların hem sisteme giriş çıkışlarının hem de etkinlik kayıtlarının (log) düzenli olarak tutulması da geçmişe yönelik siber risklerin tespiti ve incelenmesi açısından önem arz etmektedir.

• **Şifre ve Parolaların Oluşturulmasına İlişkin Önlemlerin Belirlenmesi:** Şirket çalışanları tarafından kullanılan şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilebilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmaktadır.

• **Güncel Anti-virüs Yazılımlarının Kullanılması:** Kötü amaçlı yazılımlardan korunmak için bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden anti-virüs, anti-spam gibi ürünler kullanılmaktadır. Ancak bu ürünlerin sadece kurulumunun yeterli olmaması sebebiyle güncelliklerinin sağlanmasına dikkat edilerek gerekli virüs taramaları düzenli olarak yapılmaktadır.

• **Veri Aktarımında SSL Protokolünün Kullanılması:** Veri sorumluları tarafından, farklı internet sitleri ve/veya mobil uygulama kanallarına ilişkin kişisel veri temin edilecekse, bağlantıların SSL, sFTP ya da diğer güvenli yollar ile gerçekleştirilmesine riayet edilmektedir.

• **Güvenlik Problemlerine İlişkin Raporlama Sisteminin Kurulması:** Bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zafiyet ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirilmeler yapılmaktadır.

• **Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması:** Kişisel veri içeren ortamlar tespit edilerek, saklanan kişisel verilerin güvenliğinin alınması ve verilere izinsiz erişimin engellenmesi amacıyla farklı ortamlara ilişkin tedbirler alınmaktadır.

• **Şirket Yerleşkesinde Kağıt Ortamında Saklanan Veriler:** Kağıtların çalınması veya kaybolması gibi tehditlere karşı dolap ve çekmecelerin kilit altına alınması gibi fiziksel güvenlik önlemleri alınmaktadır. Kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın,sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş çıkışların kontrol altına aınmasına

dikkat edilmektedir.

• **Elektronik Ortamında Saklanan Kişisel Veriler:** Kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılmaktadır. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alan güvenliğini sağlamak amacıyla ayılabilecektir.

• **Çalışanların Şahsi Elektronik Cihazlarının Bilgi Sistem Ağına Eişiminin Sınırlandırılması:** Çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bu cihazlara bilgi sistem ağına erişim hakkı verilmemelidir.

• **Fiziki Tedbirler:** Kişisel veri güvenliğinin sağlanması kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD, USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler alınmalıdır.

• **Fiziki Tedbirler:** Kişisel veri güvenliğinin sağlanması kişisel veri içeren kağıt ortamındaki

• **Kişisel Verilerin Bulutta Depolanması:** Kişisel verilerin bulutta depolanması, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için kimlik doğruluma kontrolünü uygulanması sağlamaktadır.

• **Email/Bilgisayar Ortamında Saklanan Kişisel Veriler:** Çalışanlara atanan email ve bilgisayarlarda saklanan kişisel verilerin minimuma indirilmesi için çalışanlar bilgilendirilmekte ve cihazların dışarıdan gelecek saldırılara karşı güvenliği sağlanmaktadır.

• **Bilgi Teknolojileri Sistemleri Tedariği, Geliştirilmesi ve Bakımı:** Kişisel veri içeren cihaz/ sistemlerin bakımının dış kaynaklı hizmetler (üretici, satıcı, servis gibi üçüncü kurumlar) tarafından gerçekleştirilecek olması durumunda kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamlarının sökülerek bakıma gönderilmesi sağlanmaktadır. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir. Belirtilen amaçlarla dışarıdan hizmet alınması durumunda, ver, güvenliğinin sağlanması amacıyla hizmet alınan şirketlerin tamamıyla KVK Kanunu m. 12/II'den kaynaklanan yükümlülüklerin yerine getirilmesi amacıyla, şirketle yapılan mevcut sözleşmeler veri güvenliğine ilişkin hükümler içerecek şekilde revize edilmektedir.

• **Kişisel Verilerin Yedeklenmesi:** Kişisel veriler içeren ortamlar belirli periyotlarla yedeklenmek suretiyle güvenlik altına alınmaktadır. Bu kapsamda;

- Yedekleme stratejilerinin oluşturulmaktadır.
- Veri seti yedeklerinin ağ dışında tutulması sağlanmaktadır.

• **Özel Nitelikli Kişisel Verilerin Saklanması:** KVK Kurulu tarafından 'Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler' ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Karar uyarınca veri Sorumlusu olarak Şirketimiz, işlenen özel niteliklli kişisel verilerin saklanmasında diğer önlemler birlikte ayrıca aşağıda belirlenmiş olan güvenlik önlemlerinin alınmasını sağlamaktadır;

- Çalışanlar İçin Yeki Matrisleri
- Erişim Loglarının Düzenli Olarak Tutulması
- Kilitlenmiş/Şifrelenmiş/Kodlanmış Sistem Girişleri
- Log kayıtlarının Kullanıcı Müdahalesinden Korunması Sağlanmaktadır.
- Özel Nitelikli Kişisel Veriler İçin güvenli şifreleme / kriptografik anahtarlar kullanılmaktadır
- Uzaktan erişimin gerektiği verilere, iki kademeli kimlik doğrulama sistemiyle erişim sağlanmaktadır.
- Verilerin bulunduğu ortamlara ait yazılımlarda güvenlik güncellemeleri takip edilmektedir.
- Yedekleme/Kademeli Kimlik Doğrulama

• **Kişisel verilerin saklanmasına ilişkin diğer tenik uygulama ve tedbirler:** İşlenen Kişisel Verilerin güvenliğinin sağlanması amacıyla Şirket bünyesinde yukarıda belirtilenlere ek olarak, genel olarak aşağıdaki tedbirler uygulanmaktadır;

- Ağ Güvenliği ve Uygulama Güvenliği
- Ağ yoluyla Kişisel Veri Aktarımlarına Kapalı Sistem AĞ
- Anahtar Yöntemi
- Bulut Sistemi Güvenliği
- Erişim Loglarının Düzenli Olarak Tutulması
- Güncel Antivirüs Sistemlerinin Kullanılması
- Güvenlik Duvarının Kullanılması
- Kişisel Verilerin Yedeklenmesi ve Güvenliğinin Sağlanması
- Kullanıcı Hesabı Yönetimi, Yetki Kontrolü ve Takibi
- Log Kaytılarının Kullanıcı Müdahalesinden Korunması
- Mevcut Risk ve Tehdit Kontrolleri

Saldırı Tespit ve Önleme Sistemleri

- Sızma Testleri
- Veri İşleyen Hizmet Sağlayıcının Veri Güvenliği Konusunda Belirli Aralıklarla Kontrolü
- Yedekleme
- Kilitlenmiş/Kodlanmış/Şifrelenmiş Sistem Girişleri
- Kilitli Dosyalama Yeri

- Güvenlik Kamerası
- Verilerin bulunduğu Ortamlara ait yazılımlarda güvenlik güncellemeleri
- Uzaktan erişimin gerektiği verilere, iki kademeli kimlik doğrulama sistemiyle erişim sağlanmaktadır.

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

KVK Kanunu madde 7 uyarınca gerçekleştirilecek olan Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi, Şirketimiz tarafından hazırlanan işbu Kişisel Verilerin Saklaması ve İmhası Talimatı'nda belirtilen esaslara uygun olarak aşağıda açıklanacak yöntemlerle gerçekleştirilmektedir.

7.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu olarak Şirketimiz silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli teknik ve idari tedbirleri almaktadır.
Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:
• Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi
• Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri işleme amacı için ilgili kullanıcıların tespit edilmesi
• İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi
• İlgili kullanıcıların kişisel veriler kapsamında erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması
Bu madde altında belirtilen yöntemler yönetmelik ve rehberde yer almakta olup, kişisel verilerin silinmesinde seçilecek yöntem Şirketimizin iç prosedürleri kapsamında ilgili olduğu ölçüde aşağıdaki tedbirler seçilmek suretiyle uygulanmaktadır;

7.1.1. Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365, Dropbox gibi) Üzerinde Bulunan Verilerin Silinmesi

Bulut sisteminde saklanan veriler silme komutu verilerek silinmektedir. Anılab işlem gerçekleştirilirken ilgili kullanıcı bulut sistemi üzerinde siliniş verileri geri getirme yetkisinin olmadığını dikkat edilmektedir.

7.1.2. Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmektedir. Karartma işlemi ilgili evreak üzerindeki kişise verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünmez hale getirilmesi şeklinde yapılır.

7.1.3. 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 gerekmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistemyöneticisi olmadığına dikkat edilmelidir.

7.1.4. Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler şifreli olarak saklanmaslı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

7.1.5. Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı koutları ile (DELETE vb.) silinmesi gerekir. Anılan bu işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.
Şirket tarafından gerçekleştirilen tüm silme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Kağıt ortamdaki kişisel verileri bakımından ise bu işlemlerin gerçekleştirildğine ilişkin tutanak düzenlenir ve ilgili birim tarafından muhafaza edilir. Elektronik ve kağıt ortamındaki kişisel verilere ilişkin silmeye ilişkin kayıtlar üç yıl süre ile saklanır.

7.2. Kişisel Verilerin Yok Edilmesi

Kişiler verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilimez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu olarak Şirketimiz silinen kişisel verilerin ilgili kullanıcılar için erişlemez ve tekrar kullanılamaz olması için gerekli teknik ve idari tedbirleri almaktadır.

Kişisel verilerin yok edilmesi, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi sağlanmaktadır.

7.2.1. Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için; Fiziksel Yok Etme yöntemi kullanılarak; Optik medya veya manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi sağlanmaktadır. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanmaktadır. Üzerine Yazma yöntemi kullanılarak; Manyetik medya ve yeniden yazılabilir optik medya üzerinde en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçirilmektedir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

7.2.2. Çevresel Sistemler

Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri; Ağ cihazları (switch, router vb.) içerisindeki sabit saklama ortamlarında yer alan veriler yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. Flash tabanlı ortamların ATA (SATA, SSD, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa uygun diğer yöntemler kullanılmak suretiyle yok edilmektedir. Mobil telefonlar (Sim kart ve sabit hafıza alanları), Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri, Veri kayıt ortamı sabit olan yazıcı gibi çevre birimleri yukarıda belirtilen yöntemlerden uygun olanları kullanmak suretiyle yok edilmektedir.

7.2.3. Kağıt Ortamlar

Şirket yerleşkeside kağıt ortamında saklanan kişisel verileri, kalıcı ve fiziksel olarak ortam üzerine yazılıdığından ana ortamınn kağıt imha veya kırpma makineleri ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde lüçük parçalara bölmek suretiyle yok edilmektedir.

7.2.4. Bulut Ortamlar

Şirket tarafından kullanılan bulut sistemlerinde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerler şifrelenmesi ve kişisel verileri için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılmaktadır.

Bulut bilişim hizmet ilişkisi sona erdiğinde, kişisel verileri kullanılmaz hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi talep edilmektedir.

7.3. Kişisel Verilerin Anonim Hale Getirilmesi

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra İlgili Kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır. Şirketimiz, kişisel verilerin anonim haline getirilmesi için saklanmakta olan Kişisel Verilerin n niteliğine ve risk-maliyet analizine göre uygun anonimleştirme yöntemlerinin belirlenmesini sağlayacaktır.

Veri sorumlusu sıfatıyla Şirketimiz, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbileri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir.

7.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan anonim hale getirme yöntemlei, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirme yöntemleridir. Bu yöntemle aşağıdaki şekildedir;

a) Değişken Çıkartma: Kişisel veri oluşturan tanımlayıcılardan birinin vey birkaçının tablodan/ sistemden bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yönetemidir. Burada dikkat edilmesi gereken, değişkenlerin çıkarılması halinde geriye kalan verilerden yola çıkarak ilgili gerçek kişinin eşleştirilemiyor olmasıdır. Örn; personel listesinin yer aldığı bir listede saklama sürelerinin dolmasının ardından yapılacak anonimleştirme uygulamsında, adrese ilişkin tanımlaycı değişkenler kaldırılsa da, kalanmaaş bilgisinden yola çıkara (söz konusu maaş miktarına şirket içerisinde tek bir kişinin sahip olması gibi) ilgili kişiye erişimin sağlanması halinde başka bir değişkenin çıkarılması yolu kullanılıcaktır.

b) Kayıtları Çıkartma: Bu yöntemde saklanmakta olan kişisel veriler arasında bir değişkenin çıkarılmasındasa tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.

c) Bölgesel Gizleme: Bu yöntemin kullanılmasında asıl amaç, kişisel verinin sahip olduğu belirleyici özellike sebebiyle kişisel verilere erişimi bulnan kişiler tarafından tahmin edilebilirliğinin önüne geçebilmek amacıyla, belirleyici özellik taşıyan veri çıkarılarak diğer veriler yerinde tutulmak suretiyle anonimleştirme sağlanmış olacaktır.

Örneğin, şirketin etkinlik katılımcı listesinde yalnızda tek bir kişinin doğum yılı 1960'tan önce ise, medeni durum, katılım bilgisi, masa numarasının birlikte saklandığı bir veri kümesinde 'doğum yılı' sekmesinin boş bırakılması suretiyle ilgili kişinin eşleştirilebilirliğinin önüne geçilecektir.

d) Genelleştirme: Bu işlem, saklanmakta olan kişisel verinin tanımlayıcı nitelikte olan belirli bir değerden, eşleştirmeyi engelleyecek daha genel bir değere çevirme işlemidir. Örneğin; performans değerlendirme raporlarının toplu bir şekilde hazırlanması durumunda, departman bilgisinin kullanılması yerine çalışanların %...'sinin belirtilerek raporun hazırlanması gerçek bir kişiye e erişmeyi imkansız hale getiren bir işlem olacaktır.

e) Al ve Üst Sınır Kodlama: Bu yöntem, belli bir değişken için kategori belirlenerek bu kategorinin içerisinde kalan değerlerin birleştirilmesi suretiyle kişisel verilerin anonim hale getirilmesi sağlanmaktadır. Örneğin; Personel listesinde yer alan kıdem ve maaşa ilişkin değişkenler belli kategorilerde gruplandırılarak (ör; 24bin TL yıllık gelirden az olanlar düşük, 5 yıldan az kıdemi olanlar junior şeklinde gruplandırılarak, ücret ve kıdem sütununun altına yeni oluşturulan değerler girilmektedir)

f) Global Kodlama: Bu yöntem, belli bir değişken için kategori belirlenerek bu yöntem rakamsal olarak gruplama yapılabilen alt ve üst sınır kodlamanın uygulanmasının mümkün olmadığı hallerde kullanılan gruplama vasıtasıyla anonim hale getirme yöntemidir. Önemli olan, veriye erişim sağlayabilen kişiler tarafından belirli değerlerin kümelenerek tahmin yürütmeyi kolaylaştırdığı hallerde kullanılır. İstenen bir veri değeri için ortak ve yeni bir grup oluşturulması suretiyle, veri kümesinde tüm kayıtlar yeni tanım ile değiştirilebilir Örneğin; müşterinin ikametgah adresi yerine semt adının yazılması.

g) Örnekleme: Bu yöntemde, veri kümesinin tamamı yerine, kişisel verileri içeren kümede yer alan bir alt kategori açıklanır veya aktarılır. Bu yöntemle ile, bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığını tahmin edilemeyeceği için veriler anonim hale getirilmiş olur. Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir ver, kümesinin anonim hale getirilerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair tahmin

yürütmek mümkün olabilecekken, söz konusu listede, sadece nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılarak, nüfus kaydı diğer illerde olan kadınlar listeden çıkarılırsa, veriye erişim sağlayan kişi, İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden kişisel veriler anonim hale getirilmiş olacaktır.

7.3.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde yukarıda belirtilenlerin aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma ortaya çıkmaktadır. Bu yöntemler kullanılırken elde edilmek istenen yarara uyumlu olacak şekilde değişkenliklerin dikkatle uygulanması gerekmektedir. Ayrıca, verilerin güncel tutulmasının KVK Kanunu kapsamında Veri Sorumlusuna yüklenmiş olan bir kural olduğu düşünüldüğünde, değer düzensizliği sağlanması halinde ilgili kişinin gerçeğe aykırı bir hale geldiği durumlarda söz konusu yöntemler uygulanmaktadır.

a) Mikro Birleştirme: Bu yöntem ile kişisel veri içeren veri kümesindeki bütün kayıtlar ilk olarak anlamlı bir sıraya göre dizilerek, sonrasında bütün kümenin belirli bir sayıda alt kümelere ayrılması sağlanır. Sonrasında, her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkene ait değeri ortalama değer ile değiştirilir. Bu şekilde, değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir. Örneğin; Kıdem süresi 5 yıldan az, 5-10 yıl arası ve 15 yıldan fazla olan kişler tespit edilerek, kıdem yılları kişi sayısına bölünmek suretiyle, kıdem süresinin ortalaması alınır, sonrasında kıdem yılı yerine her bir kıdem aralığında bulunan kişi için, o kıdem aralığında çıkan ortalama değer yazılmak suretiyle anonimleştirme sağlanmış olur.

b) Veri Değiş Tokuşu: Bu yöntem, kişisel veri içeren akyıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem teel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve asıl amaç değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesi suretiyle anonim hale getşrme sürecinin sağlanmasıdır.

c) Gürültü Ekleme: Bu yöntem, genel olarak sayısal verilerin bulunduğu bir ver kümesinde uygulanmakta olup, mevcut verilere belirlenen oranda artı veya eksi yönde birakım sapmalar eşit ölçüde eklenerek veriler anonim hale getirilebilmektedir. Örneğin, maaş bilgilerinin yer aldığı listede tüm personellerin maaşına ayrı ayrı eşit ölçüde değer eklenip/çıkarılarak anonim hale getirme sağlanmış olur.

d) İstatiksel Yöntemler: Anonim hale getirilmiş veri kümelerinde çeşitli istatiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonim hale getirme süreci güçlendirmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirmek suretiyle, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

7.3.2. Anonimlik Güvencesi

Şirketimiz tarafından, saklanmakta olan kişisel verilerin saklama sürelerinin dolmasının ardından silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların sağlanmış olduğunun kontrolü gerçekleştirilmektedir;

- Anonim hale getirilmiş bir veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğinin bozulmaması,
- Bir yada birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Şirketimiz yukarıda sayılan ihtimallerin ortadan kaldırılması amacıyla, Şirketimiz tarafından anonim hale getirilen veri kümeleri üzerinde bu maddede sayılan özellikler değiştikçe kontroller gerçekleştirerek, anonimliğin korunduğudan emin olmak için gerekli tedbirleri yerine getirmeye çalışmaktadır.

8.0 KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

KVK Kanunu kapsamında Veri Sorumlularının yerine getirmesi gereken birçok yükümlülük bulunması ve Kişisel Verilerin İşlenmesi ve Hukuka Uygun Olarak Korunması yaşayan ve sürekli takip edilmesi gereken bir süreç olduğundan dolayı Veri Sorumlusu olarak Şirketimiz gerekli tedbirleri almaktadır.

Bu doğrultusa, Avcı Kalıp Sac Metal Makine San.Tic.Ltd.Şti., kişisel verilerin işlenmesine, saklanması ve imhasına yönelik süreçlerin takibi, KVK Kanunu'na uyumluluğun sağlanması ve faaliyetlerinin KVK Kanunu'na uygun olarak yerine getirilebilmesi içi, Genel Müdür Kararı ile bünyesinde bir Kişisel Veri Koruma Komitesi (KVK Komitesi) oluşturmuştur.

KVK Komitesi'nin başlıca görevleri;

- Mevzuat uyarınca yükümlülüklerini yerine getiren veri sorumlusuna, veri işleyene ve

çalışanlara bilgi vermek ve tavsiyede bulunmak,
- Veri sorumlusunun kişisel verilerin korunması ile ilgili talimatlarının yanı sıra kişise veri işlemede yer alan çalışanların bilinçlendirilmesi ve eğitilmesi ve ilgili denetimlerin mevzuata uygunluğunu takip etmek
- Kendisine yüklenen görevlerini yaparken, görevlerin yerine getirilebilmesi için gerekli parasal ve fiziksel kaynakları belirlemek, kişisel verilere ve işlemlere erişebilmesini sürdürebilmek,
- Belirlenen temel politika ve aksiyon adımlarını üst yönetimin onayına sunmak, uygulamasını gözetmek ve koordinasyonunu sağlamak,
- Kişisel verilerin korunması konusundaki gelişmeleri takip etmek ve bu gelişmeler kapsamında yapılması gerekenler konusundaki gelişmeleri takip etmek ve bu gelişmeler kapsamında yapılması gerekenler konusunda üst yönetime tavsiyelerde bulunmak,
- İlgili kişilerin berilerinin hukuka, Kişisel Verilerin İşlenmesi ve Koruması Talimatına ve Kişisel Verilerin Saklanması ve İmhası Talimatına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemek,
- Şirket, Genel Müdür'ün kişisel verilerin korunması ile ilgili süreçlere yönelik olarak vereceği talimatları ve görevleri yerine getirmek ile yetkili ve görevlidir.

Bununla birlikte, Avcı Kalıp bünyesinde kişisel veri işleyen tüm departmanların sorumluları/ yöneticileri, gerek kendş departmsanlarının kişisel veri işleme envanterinin güncelliğinin sağlanması gerek kişisel veri saklama ve imha süreçlerinin takibi için bölümünde çalışan bir başka kişiyi görevlendirebilecektir.

Avcı Kalıp KVK Komitesinde yer alan çalışanların unvan, birim ve görevlerine ilişkin bilgiler aşağıda yer almaktadır.

UNVAN	DEPARTMAN	SORUMLULUK
Kalite Güvence Uzmanı (İrtibat Kişisi)	Kalite Departmanı Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ve görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

Satınalma ve Muhasebe Müdürü	Satınalma Departmanı Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanmasının yönetimi ve görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

9.0 SAKLAMA VE İMHA SÜRELERİ TABLOSU

Saklama ve imha süreleri tablosuna her bir departman bazında hazırlanmıştır Kişisel Veri İşleme Envanteri'nde yer verilmekte olup, işbu envantede süreç bazında belirtilen süreler ile ilgili özel tablo aşağıda yer almaktadır.

Bu kapsamda işlenen kişisel veriler, akine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça işbu Saklama ve İmha Talimatı'nda belirtilen hususlar dikkate alınarak aşağıdaki tabloda beliritlen süreler boyunca saklanacak, süre sonunda ise imha edilecektir.

Kişisel Verileri Saklama ve İmha Süreleri'ni gösteren tablo kişisel veri işleme envanterinde yer alan süreçllerin yürütülmesinden sorumlu departmanlarca, tereddüt halinde KVK Komitesi değerlendirmeleri de alınarak güncellenecebilecektir.

Şirket tarafından yürütülen iş süreçlerinin etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin kategorisi, kişisel verilerin yer aldığı ortamların özelliği ve ilgili kullanıcı tarafından dikkate alınarak ilgili uzman tarafından yapılacaktır.

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
İş Kanunu kapsamında saklanan veriler (ör; Kıdem tazminatı, İhbar tazminatı, Kötüniyet tazminatı, Eşit Davranma İlkesine aykırılık tazminatına konu olabilcek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	İş ilişkisinin sona ermesinde itibaren 5 yıl	4877 Satılı İş Kanunu ve İlgili mevzuat	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Kanunu kapsamında saklanan özlük dosyasına ilişkin veriler (ör;Kıdem tazminatı, İhbar tazminatı, Eşit Davranma İlkesine aykırılık tazminatı dışındaki taleplere konu olabilecek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	İş ilişkisinin sona ermesinde itibaren 10 yıl	4857 Satılı İş Kanunu ve İlgili mevzuat/6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 6 ay içerisinde
Iş Kanunu kapsamında saklanan verilerden Sendikal tazminata konu olabilecek veriler (ör; performans kayıtları, disiplin cezaları, fesih evrakları vs.)	İş ilişkisinin sona ermesinde itibaren 10 yıl	6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (ör; işe giriş sağlık testleri, sağlık raporları, isg eğitimleri, iş sağlığı ve güvenliği faaliyetlerine ilişkin kayıtlar vs.)	İş ilişkisinin sona ermesinde itibaren 15 yıl	6331 sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği	Saklama süresinin bitimini takiben 6 ay içerisinde
SGK mevzuatı kapsamında tutulan veriler; (ör; işe giriş bildirgeleri, prim/hizmet belgeleri)	İş ilişkisinin sona ermesine müteakip 10 yıl	5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve İlgili mevzuat	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Kanunu uyarınca; çalışan ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	4357 Sayılı İş Kanunu ve İlgili mevzuat	Saklama süresinin bitimini takiben 180 gün içerisinde

Çalışan Erişim Kısıtlamaları İşlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	4357 Sayılı İş Kanunu ve İlgili mevzuat	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler (ör; huzur hakkı ödemesi, kar payı)	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler (pay defterinde yer alan kişisel veriler)	Pay defterinin saklanma zorunluluğu sebebiyle Süresiz	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Avans Ödemesi	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
İş Başvurusu kabul edilmediği takdirde Aday Başvurularına ilişkin veriler (ör; CV, Cover Letter, Başvuru Formu vs.)	1 yıl	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Sendikal faaliyetler uyarınca işlenen ve sendika ile paylaşılan kişisel veriler	10 yıl	6356 Sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara Yönelik Kurumsal İletişim Faaliyetleri uyarınca işlenen veriler (ör; Katılımcı Listesi)	İş ilişkisinin sona ermesine müteakip 10 yıl	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Memnuniyet Anketlerine İlişkin Veriler	İş ilişkisinin sona ermesine müteakip 10 yıl	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde

Şirket faaliyetleri uyarınca, saklanması gereken ticari defterler, ticari defterlerde yer alan kayıtlara dayanak oluştural belgeler, finansal tablolar, vs. uyarınca işlenebilecek kişisel veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Genel Kurul İşlemleri uyarınca işlenen veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirketin taraf olduğu sözleşmelerin kurulması ve içeriğine ilişkin kişisel veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Mal ve hizmetleri tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerde tanınırlığı artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderilen ticari elektronik iletilere ilişkin onay kayıtları	1 yıl	29417 sayılı 15.07.2015 tarihli Resmi Gazete'de yayımlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	Saklama süresinin bitimini takiben 180 gün içerisinde
Mal ve hizmetleri tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerde tanınırlığı artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderilen ticari elektronik iletilere ilişkin onay kayıtları dışındaki veriler	1 yıl	29417 sayılı 15.07.2015 tarihli Resmi Gazete'de yayımlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	Saklama süresinin bitimini takiben 180 gün içerisinde
Vergisel kayıtlara ilişkin kişisel veriler	5 yıl	213 sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde

Fatura/Gider pusulası/Makbuz gibi Vergi Usul Kanunu uyarınca tutulması gereken belgelerle işlenen kişisel veriler	5 yıl	213 sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Ziyaretçilerin Kişisel Verileri	2 yıl	214 sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takiben 180
Kamera kayıtları gibi güvenlik amaçlı olarak işlenen kişisel veriler	90 gün	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri Bilgilerinden, TTK md.28 uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesine ilişkin kişisel veriler	10 yıl	6102 Sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri İşlem Bilgileri Müşterilerin Talep/Şikayet/Önerilerine ilişkin Çağrı kayıtları vs.)	10 yıl	6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde

10.0 PERİYODİK İMHA SÜRESİ

Avcı Kalıp saklama süresi sona eren ve kişisel verinin saklanmasını gerektirecek başka herhangi bir vei işleme amacı mevcut olmayan kişisel verileri, saklama süresinin sona ermesini takiben 180 gün (6 ay) içerisinde anonim hale getirir.

11.0 İLGİLİ KİŞİNİN TALEP ETMESİ DURUMUNDA KİŞİSEL VERİLERİN SİLME VE YOK ETME SÜRELERİ

İlgili kişi, Avcı Kalıp'a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde, Şirketimiz;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri işbu talimat uyarınca siler, tok eder veya anonim hale getirir. Şirket, ilgili kişilerin silme veya yok etme taleplerini en geç 'otuz gün' içinde sonuçlandırır.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa; bu durumda aktarım yapılan üçüncü kişiye bildirerek söz konusu kişisel verilerin silinmesi veya yok edilmesini talep eder.
Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Kişisel Verilerin Korunması Kanunu'nun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 'otuz gün' içinde, ilgili kişinin talebine uygun olarak, yazılı olarak ya da elektronik ortamda bildirilir.

12.0 KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI TALİMATINDA YAPILACAK GÜNCELLEMELER

Şirket, KVK Kanunu'nda yapılan değişiklikler nedeniyle, KVK Kurumu kararları uyarınca ya da ortaya çkacak gelişmeler doğrultusunda, Kişisel Verilerin İşlenmesi ve Korunması Talimatı'nda ya da işbu Kişisel Verilerin Saklanması ve İmhası Talimatı'nda değişiklik yapma hakkını saklı tutmaktadır.
İşbu Kişisel Verilerin Saklanması ve İmhası Talimatı'nda yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar talimatın sonunda açıklanır. İşbu talimatta yapılacak güncellemeler Şirket tarafından onaylanması üzerine revizyon ve onay tarihi ile birlikte tüm bölüm ve departmanlara e-posta üzerinden dağıtımı yapılır.

13.0. YÜRÜRLÜK

İşbu Kişisel Verilerin İşlenmesi ve Korunması Talimatı ve ileride yapılacak güncellemeler, e-posta ve yazılı metin olarak tüm çalışanlarımızın erişimine sunulucaktır.