

 Otomotiv Mam�lleri San. ve Tic.Ltd.Őti.	<b>KİŐİSEL VERİLERİN KORUNMASI</b>	Versiyon	<b>1.0</b>
		İlk Yayın Tarihi	<b>13.04.2021</b>
	KiŐisel Verilerin Saklanması ve İmha Politikası	Son G�ncelleme Tarihi	
	Sayfa No	<b>1 / 27</b>	

## MERVAN OTO. MAM. SAN. VE TİC. LTD. ŐTİ.

### KİŐİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI

#### İÇİNDEKİLER TABLOSU

<b>1. GİRİŐ</b> .....	<b>2</b>
<b>2. Amaç ve Kapsam</b> .....	<b>2</b>
<b>3. Tanımlar</b> .....	<b>3</b>
<b>4. Politika İle D�zenleme Altına Alınan Kayıt Ortamları</b> .....	<b>5</b>
<b>5. KiŐisel verilerin saklanması ve imhasını gerektiren hukuki, teknik ya da diŐer sebepler</b> .....	<b>5</b>
<b>6. KiŐisel verilerin g�venli bir Őekilde saklanması ile hukuka aykırı olarak iŐlenmesi ve eriŐilmesinin �nlenmesi iin alınmıŐ teknik ve idari tedbirler</b> .....	<b>7</b>
6.1. İdari Tedbirler .....	7
6.2. Teknik Tedbirler.....	9
<b>7. KiŐisel verilerin hukuka uygun olarak imha edilmesi iin alınmıŐ teknik ve idari tedbirler</b> .....	<b>12</b>
7.1. KiŐisel Verilerin Silinmesi .....	13
7.2. KiŐisel Verilerin Yok Edilmesi .....	14
7.3. KiŐisel Verilerin Anonim Hale Getirilmesi.....	15
<b>8. KiŐisel verileri saklama ve imha s�relerinde yer alanların unvanları, birimleri ve g�rev tanımları</b> .....	<b>20</b>
<b>9. Saklama ve imha s�releri tablosu</b> .....	<b>21</b>
<b>10. Periyodik imha s�resi</b> .....	<b>26</b>
<b>11. İlgili KiŐinin talep etmesi durumunda kiŐisel verilerin silme ve yok etme s�releri</b> .	<b>26</b>
<b>12. KiŐisel Verilerin Saklanması ve İmhası Politikasında yapılacak G�ncellemeler</b> ....	<b>26</b>
<b>13. Y�R�RL�K</b> .....	<b>27</b>

## 1. 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 olarak bekleyen 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.

Mervan Otomotiv Mam. 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 Politikası, Mervan Otomotiv Mam. San. Tic. Ltd. Şti tarafından yürürlüğe konulmuştur.

## 2. AMAÇ VE KAPSAM

İşbu Kişisel Verilerin Saklanması ve İmhası Politikasının ("Saklama ve İmha Politikası") amacı; Mervan Otomotiv Mam. San. Tic. Ltd. Şti. ("Şirket") tarafından tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlenen kişisel verilerin işleme sürelerinin belirlenmesi ve işleme süresi ve/veya işleme amacı ortadan kalkan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ("kişisel verilerin imhası") ilişkin usul ve esasların belirlenmesidir.

İşbu Saklama ve İmha Politikası'nda, 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkındaki Yönetmeliğin ("Yönetmelik") 6'ncı 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 ve Anonim Hale Getirilmesi Rehberi de bu çerçevede KVKK tarafından yayımlanan diğer tüm dökümanlar dikkate alınarak hazırlanmıştır.

İşbu Saklama ve İmha Politikası, KVK Kanunu'nun 7'nci maddesi uyarınca "veri sorumlusu" sıfatıyla Mervan Otomotiv Mam. San. Tic. Ltd. Şti'nin çalışan adaylarından, çalışanlarından, eski çalışanlarından, gerçek kişi iş/çözüm ortaklarından, iş/çözüm ortağı yetkilisi ve çalışanlarından, tedarikçilerinden, hissedar ve ortaklarından, stajyerlerinden, stajyer adaylarından ve ziyaretçilerinden tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlediği, elektronik

ortalarda, kağıt ortamlarda ve işbu Politika'da belirtilen diğer kayıt ortamlarında yer alan ve işleme şartları sona ermiş tüm Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini kapsamaktadır.

### 3. TANIMLAR

<b>Açık Rıza</b>	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
<b>Alıcı Grubu</b>	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini
<b>Anonim Hale Getirme</b>	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
<b>İlgili Kullanıcı</b>	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.
<b>KVKK/KVK Kanunu</b>	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
<b>Kayıt Ortamı</b>	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.
<b>Kişisel Veri</b>	Kimliği belirli veya belirlenebilir gerçek kişiyle eşleştirilebilen her türlü bilgi.
<b>Kişisel Verilerin İmhası</b>	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
<b>Kişisel Verilerin İşlenmesi</b>	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.
<b>Kişisel Verilerin Silinmesi</b>	Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
<b>Kişisel Verilerin Yok Edilmesi</b>	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
<b>KVK Kurulu</b>	Kişisel Verileri Koruma Kurulu.
<b>KVK Kurumu</b>	Kişisel Verileri Koruma Kurumu
<b>Özel Nitelikli Kişisel Veri</b>	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte “Kişisel Veriler” olarak adlandırılacaktır.
<b>Periyodik İmha</b>	Kanun’da yer alan kişisel verilerin işleme 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.
<b>Veri İşleyen</b>	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
<b>Veri Kayıt Sistemi</b>	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
<b>Veri Sahibi/İlgili Kişi</b>	Kişisel verisi işlenen gerçek kişi

<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
-----------------------	---

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

#### 4. POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI

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 kayıt ortamı olarak adlandırılmaktadır. Bu ortamlar genel olarak aşağıdaki gibidir;

- **Fiziki Ortamlar:** Kişisel Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
- **Yerel dijital ortamlar:** Şirket bünyesinde yer alan bilgisayarlar, sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır.
- **Bulut ortamlar:** Şirket bünyesinde yer almamakla birlikte, Şirket'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

Yukarıda sayılan kayıt ortamlarının yanında, Şirket tarafından işlenen Kişisel Veriler aşağıda belirtilen ve ileride ortaya çıkabilecek kayıt ortamlarında da saklanabilecektir;

- Ağ cihazları,
- Mikrofiş,
- Yazıcı, Parmak izi okuyucu gibi çevre birimler,
- Flash hafızalar.

#### 5. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK YA DA DİĞER SEBEPLER

Mervan Otomotiv Mam. San. Tic. Ltd. Şti bünyesindeki çeşitli departmanlar tarafından iş tanımları doğrultusunda yürütülen iş süreçleri ve bu süreçlere bağlı faaliyetleri gerçekleştirebilmek amacıyla çalışanlarının, çalışan adaylarının, eski çalışanlarının, gerçek kişi iş/çözüm ortaklarının, iş/çözüm ortaklarının çalışanları ve yetkililerinin, tedarikçilerinin, hissedar ve ortaklarının, stajyerlerinin, stajyer adaylarının ve ziyaretçilerinin olmak üzere farklı ilgili kişi kategorilerine ait kişisel verileri işlemektedir.

KVK Kanunu md.5'te yer alan işleme 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 saklanmaktadır.

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 bulunan İlgili Kişilerin, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunması veya rızasına hukuki geçerlik tanınmaması sebebiyle, kendisinin veya bir başkasının hayatı ve beden bütünlüğünün korunabilmesi için saklanmasının zorunlu olması
- e) Kişisel verilerin Şirket'in yerine getirmekte olduğu faaliyetler kapsamında 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 hak 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 Politika'da 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 şikâyette bulunulması 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. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

KVK Kanununun 12nci maddesinin birinci fıkrasında; Veri Sorumlusu'nun; (i) Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek, (ii) Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek, (iii) 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 belirtilen sebeplerle saklanmakta olan Kişisel veriler için başlıca aşağıdaki idari ve teknik tedbirler alınmıştır.

### 6.1.İdari Tedbirler

- **Mevcut risk ve tehditlerin belirlenmesi:** Şirket tarafından Kişisel Veri İşleme Envanteri hazırlanarak, işlenen kişisel verilerin kategorileri, işleme amacı, aktarıldığı alıcı grupları, saklama süreleri, verisi işlenen ilgili kişi grubu belirlenerek 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 politikaların değişmesi halinde, yeni politikalara uyum sağlamak amacıyla verilen eğitimler tekrarlanmaktadır.
- **Kişisel verilerin güvenliğine ilişkin politikalara uyumun sağlanması:** KVK Kanunu kapsamında veri sorumlusu sıfatıyla Şirket olarak hazırlamakla yükümlü olduğumuz politikaların yanı sıra Şirket çalışanlarına yönelik olarak gizlilik politikaları revize dilmekte ve iç etik kuralları, bilgi güvenliği politikası gibi metinler kanun kapsamında revize edilerek uyulması gereken usul ve yasaklar hakkında çalışanlar bilgilendirilmektedir.
- **Minimum veri işleme:** Veri Sorumlusu sıfatıyla Şirket'in kişisel veri işleme amaçları çerçevesinde en az sayıda veri işlenmesi sağlanmakta ve işlenme ihtiyacı duyulmayan veriler de kişisel veri saklama ve imha politikası 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 bulunan iş ortaklarımız, tedarikçilerimiz, 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 muhafazası ve güvenliği sağlanmaktadır.
- **Kişisel verilerin işlenmesi prosedürlerinin 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 ilişkin denetimler:** Şirket, KVK Kanunu hükümlerinin uygulanmasını sağlamak amacıyla gerekli iç denetimleri yapmaktadır.
- **Kişisel verilerin saklanmasıyla ilgili 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 Politikaların Oluşturulması
  - Gizlilik Taahhütnamelerinin Alınması
  - Sözleşmelerde Veri Güvenliğine İlişkin Hükümlerin Eklenmesi
  - Kişisel Veri Güvenliği, Politika 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 Politika 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 modüllerinin 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.
  - Tüm çalışan personellerin kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlanmaktadır.
  - Kaba kuvvet algoritması (BFA) 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 ilişkin önlemlerin belirlenmesi:** Şirket çalışanları tarafından kullanılan şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek 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 da dikkat edilerek gerekli virüs taramaları düzenli olarak yapılmaktadır.
- **Veri aktarımlarında SSL protokolünün kullanılması:** Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL, sFTP ya da diğer güvenli yollar ile gerçekleştirilmesine riayet edilmektedir.
- **Güvenlik problemlerine ilişkin raporlama sisteminin kurulması:** Bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak *zafiyet taramaları* ve *sızma testlerinin* yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler 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 yerleşkelerinde kâğıt ortamında saklanan veriler:** kâğıtların çalınması veya kaybolması gibi tehditlere karşı dolap ve çekmecelerin kilit altına alınması gibi fiziksel güvenlik önlemler alınmaktadır. Kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınmasına dikkat edilmektedir.
- **Elektronik ortamda 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 alanın güvenliğini sağlamak amacıyla ayrılabilir.
- **Çalışanların şahsi elektronik cihazlarının bilgi sistem ağına erişiminin sınırlandırılması:** Çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bu cihazlara bilgi sistem ağına erişim hakkı verilmemektedir.
- **Fiziki tedbirler:** Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması (arşiv odası), kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler alınmaktadır.
- **Kişisel verilerin bulutta depolanması:** yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması sağlanmaktadır.

- **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 tedarigi, geliştirmesi 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, veri güvenliğinin sağlanması amacıyla hizmet alınan şirketlerin tamamıyla KVK Kanunu m. 12/II'den kaynaklanan yükümlülüklerin yerine getirilmesi amacıyla, şirketlerle yapılan mevcut sözleşmeler veri güvenliğine ilişkin hükümler içerecek şekilde revize edilmektedir.
- **Kişisel Verilerin Yedeklenmesi:** Kişisel veriler içeren ortamlar belirli periyotlarla yedeklemek suretiyle güvenlik altına alınmaktadır. Bu kapsamda;
  - Yedekleme stratejilerinin oluşturulmaktadır.
  - Veri seti yedeklerinin ağ dışında tutulması sağlanmaktadır.
- **ISO 27001 Standardının uygulanması:** Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Veri Güvenliği Rehberi'nde de yer alan bu hususların sistematik bir şekilde Şirket bünyesinde yerine getirilebilmesi ve rehberde bahsi geçmeyen hususlardaki bilgi güvenliğinin sağlanması amacıyla Şirket bünyesinde, ISO 27001 adlı TSE standardında yer alan tedbirler mümkün olduğu ölçüde yerine getirilmeye çalışılmakta ve gerekli yatırımlar yapılmaktadır.
- **Özel Nitelikli Kişisel Verilerin saklanması:** KVK Kurulu tarafından yayımlanan "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 nitelikli kişisel verilerin saklanmasında diğer önlemlerle birlikte ayrıca aşağıda belirlenmiş güvenlik önlemlerinin alınmasını sağlamaktadır;
  - Çalışanlar İçin Yetki Matrisleri
  - Erişim Loglarının Düzenli Olarak Tutulması
  - Kilitlenmiş/kodlanmış/şifrelenmiş 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 teknik uygulama ve tedbirler:** İşlenen Kişisel Verilerin güvenliğinin sağlanması amacıyla Şirket bünyesinde yukarıda belirtilenlere ek olarak, genel olarak aşağıdaki teknik tedbirler uygulanmaktadır;
  - Ağ Güvenliği ve Uygulama Güvenliği
  - Ağ Yoluyla Kişisel Veri Aktarımlarında Kapalı Sistem Ağ
  - Anahtar Yöntemi
  - Bilgi Teknolojileri Sistemleri Kapsamındaki Güvenlik Önlemleri
  - Bulut Sistemi Güvenliği
  - Erişim Loglarının Düzenli Olarak Tutulması
  - Veri Maskeleyme
  - Güncel Antivirüs Sistemlerinin Kullanılması
  - Güvenlik Duvarının Kullanılması
  - Kağıt Yoluyla Aktarılan Verilerin Gizlilik Sınıflandırılmasının Uygulanması
  - Kişisel Verilerin Yedeklenmesi ve Güvenliğinin Sağlanması
  - Kullanıcı Hesabı Yönetimi, Yetki Kontrolü ve Takibi
  - Log Kayıtlarının Kullanıcı Müdahalesinden Korunması
  - Mevcut Risk ve Tehdit Kontrolleri
  - Saldırı Tespit ve Önleme Sistemleri Kullanılmaktadır
  - Sızma Testleri
  - Siber Güvenlik Tedbirlerinin Alınması ve Takibi
  - Şifreleme ve Otomatik Şifre Güncelleme Uygulanmaktadır
  - Veri İşleyen Hizmet Sağlayıcının Veri Güvenliği Konusunda Belirli Aralıklarla Kontrolü
  - Veri Kaybı Önleme Yazılımları (DLP)
  - Yedekleme
  - Kilitlenmiş/kodlanmış/şifrelenmiş sistem girişleri
  - Kilitli Dosyalama Yeri/Arşiv Odası/Kasalar
  - Sistem Odası/Arşiv Güvenlik Kamerası
  - Verilerin bulunduğu ortamlara ait yazılımlarda güvenlik güncellemeleri
  - Uzaktan erişimin gerektiği verilere, iki kademeli kimlik doğrulama sistemiyle erişim sağlanmaktadır.

## **7. 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 Saklanması ve ve İmhası Politikası'nda belirtilen esaslara uygun olarak aşağıda açıklanacak yöntemlerle gerçekleştirilmektedir.

Mervan Otomotiv Mam. San. Tic. Ltd. Şti işlediği kişisel verilerin hukuka uygun olarak imha edilmesini sağlamak amacıyla Şirket nezdinde Veri İmha Sorumlusu belirlenmiştir. Veri İmha Sorumlusu; işlenen kişisel verinin özelliğine, kişisel verilerin saklanma amacına ve kişisel verilerin saklanmakta olduğu ortamlara uygun olacak şekilde aşağıdaki yöntemlerden gerekli olanı uygulamaktadır.

### **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. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmektedir.

#### **7.1.2. Kağıt Ortamında Bulunan Kişisel Veriler**

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmektedir. Karartma işlemi ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak

şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde 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 sistem yöneticisi olmadığına dikkat edilmelidir.

### **7.1.4. Taşınabilir Medyada Bulunan Kişisel Veriler**

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

### **7.1.5. Veri Tabanları**

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

Şirketimiz tarafından gerçekleştirilen tüm silme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Kağıt ortamdaki kişisel veriler bakımından ise bu işlemlerin gerçekleştirildiğine ilişkin tutanak düzenlenir ve Teknik Birim tarafından muhafaza edilir. Elektronik ve kağıt ortamdaki kişisel verilere ilişkin silmeye ilişkin kayıtlar üç yıl süre ile saklanır.

## **7.2. Kişisel Verilerin Yok Edilmesi**

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

Kişisel verilerin yok edilmesi için, 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; (i) Fiziksel Yok Etme yöntemi kullanılarak; Optik medya ve 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. (ii) Üzerine Yazma yöntemi kullanılarak; Manyetik medya ve yeniden yazılabilir optik medya üzerine en yaz yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmektedir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

### **7.2.2. Çevresel Sistemler**

Ortam türüne bağlı olarak kullanılabilir yok etme yöntemleri; (i) Ağ cihazları (switch, router vb.) içerisindeki sabit saklama ortamlarında yer alan veriler yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. (ii) 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. (iii) Mobil telefonlar (Sim kart ve sabit hafıza alanları), (iv) Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri, (v) Veri kayıt ortamı sabit olan yazıcı gibi çevre birimleri yukarıda belirtilen yöntemlerden uygun olanları kullanmak suretiyle yok edilmektedir.

### **7.2.3. Kağıt Ortamlar**

Şirket yerleşkesinde kağıt ortamında saklanan kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazıldığı olduğundan ana ortamın kağıt imha veya kırma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek suretiyle yok edilmektedir.

### **7.2.4. Bulut Ortamı**

Şirket tarafından kullanılan bulut sistemlerinde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler 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 kullanılamaz 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 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 tedbirleri 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 yöntemleri, 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 anonimleştirmeye yöntemleridir. Bu yöntemler aşağıdaki şekildedir;

#### **a) Değişken Çıkartma:**

Kişisel verileri oluşturan tanımlayıcılardan birinin veya birkaçının tablodan/sistemden bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir.

Burada dikkat edilmesi gereken, değişkenlerin çıkarılması halinde geriye kalan verilerden yola çıkarak ilgili gerçek kişinin eşleştiremiyor olmasıdır. Örn; personel listesinin yer aldığı bir listede saklama sürelerinin dolmasının ardından yapılacak anonimleştirme uygulamasında, adrese ilişkin tanımlayıcı değişkenler kaldırılrsa da, kalan maaş bilgisinden yola çıkarak (söz konusu maaş miktarına şirket içerisinde tek bir kişinin sahip olması gibi) ilgili kişiye erişimin sağlanması halinde bir başka değişkenin çıkarılması yolu kullanılacaktır.

#### **b) Kayıtları Çıkartma:**

Bu yöntemde saklanmakta olan kişisel veriler arasında bir değişkenin çıkarılmasındansa tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.



Örneğin, burs listesinde herhangi bir üniversiteden/okuldan yalnızca tek bir kişinin yer alması durumunda tüm listeden okul adı değişkenini çıkartmaktansa, bu kişiye ait satırın tümü çıkartılacaktır.

**c) Bölgesel Gizleme:**

Bu yöntemin kullanılmasında asıl amaç, kişisel verinin sahip olduğu belirleyici özellik sebebiyle kişisel verilere erişimi bulunan 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 yalnızca 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 erişmeyi imkansız hale getiren bir işlem olacaktır.

**e) Alt ve Üst Sınır Kodlama:**

Bu yöntem, belli bir değişken için bir 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 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 kümesindeki tüm kayıtlar yeni tanım ile değiştirilmektedir.

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 yöntem ile, bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığının tahmin edilemeyeceği için veriler anonim hale getirilmiş olur.

Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesinin anonim hale getirilerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair tahmin yürütmek mümkün olabileceksen, 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 verilerinin gerçeğe aykırı bir hale geldiği durumlarda söz konusu yöntemler uygulanmamalıdır.

#### **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 değişkenine 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 kişiler 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 kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeyle ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve asıl amaç değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesi suretiyle anonim hale getirme sürecinin sağlanmasıdır.

**c) Gürültü Ekleme:**

Bu yöntem, genel olarak sayısal verilerin bulunduğu bir veri kümesinde uygulanmakta olup, mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eşit ölçüde eklenerek veriler anonim hale getirilmektedir.

Örneğin, maaş bilgilerinin yer aldığı listede tüm personelin maaşına ayrı ayrı eşit ölçüde değer eklenip/çıkarılarak anonim hale getirme sağlanmış olur.

**d) İstatistiksel Yöntemler:**

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

**7.3.3. 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 anonimliğin bozulmaması,
- Bir ya da birden fazla değer bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,
- 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 değişikçe kontroller gerçekleştirerek, anonimliğin korunduğundan emin olmak için gerekli tedbirleri yerine getirmeye çalışmaktadır.

## **8. KİŞİSEL VERİLERİ 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 doğrultuda, Mervan Otomotiv Mam. 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 için, Şirketin Yönetim Kurulu 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 çalışanlarına bilgi vermek ve tavsiyede bulunmak,
- Veri sorumlusunun kişisel verilerin korunması ile ilgili politikalarının yanı sıra kişisel 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 veri sahiplerinin başvurularını hızlı bir şekilde karşılayacak bir mekanizma oluşturmak ve başvuruları en üst düzeyde karara bağlamak,
- Kişisel verilerin korunması konusundaki gelişmeleri takip etmek ve bu gelişmeler kapsamında yapılması gerekenler konusunda üst yönetime tavsiyelerde bulunmak,
- İlgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Verilerin Saklanması ve İmhası Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemek,

- Şirket, Yönetim Kurulu'un kişisel verilerin korunması ile ilgili süreçlere yönelik olarak vereceği talimatları ve görevleri yerine getirmek ile yetkili ve görevlidir.

Bununla birlikte, Mervan Otomotiv Mam. San. Tic. Ltd. Şti., bünyesinde kişisel veri işleyen tüm departmanların sorumluları/yöneticileri, gerek kendi departmanlarının kişisel veri işleme envanterinin güncelliğinin sağlanması gerek kişisel veri saklama ve imha süreçlerinin takibi için bölümünde çalışan bir başka kişiyi görevlendirebilecektir.

## 9. SAKLAMA VE İMHA SÜRELERİ TABLOSU

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

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

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

Şirket tarafından yürütülen iş süreçlerini 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 Bilgi Teknolojileri departmanı uzmanı tarafından yapılacaktır.

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
İş Kanunu kapsamında saklanan veriler (örn; Kıdem tazminatı, İhbar tazminatı, Kötüniyet tazminatı, Eşit Davranma İlkesine aykırılık tazminatına konu olabilecek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	İş ilişkisinin sona ermesinden itibaren 5 yıl	4857 Sayılı İş Kanunu ve ilgili mevzuat	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Kanunu kapsamında saklanan özlük dosyasına	İş ilişkisinin sona erdiği	4857 Sayılı İş Kanunu ve ilgili	Saklama süresinin

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
ilişkim veriler (örn; Kıdem tazminatı, İhbar tazminatı, Kötüniyet tazminatı, Eşit Davranma İlkesine aykırılık tazminatı dışındaki taleplere konu olabilecek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	tarihten itibaren 10 yıl	mevzuat/6098 sayılı Türk Borçlar Kanunu	bitimini takiben 6 ay içerisinde
İş Kanunu kapsamında saklanan verilerden Sendikal tazminata konu olabilecek veriler (örn; performans kayıtları, disiplin cezaları, fesih evrakları vs.)	İş ilişkisinin sona ermesinden 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, iş eğitimi, iş sağlığı ve güvenliği faaliyetlerine ilişkin kayıtlar vs.)	İş ilişkisinin sona ermesinden 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 (örn; işe giriş bildireleri, prim/hizmet belgeleri)	İş ilişkisinin sona ermesine müteakip 10 yıl	5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve ilgili 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 ilgili mevzuat	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Erişim Kısıtlamaları-Active Directory işlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	4357 Sayılı İş Kanunu ve ilgili mevzuat	Saklama süresinin bitimini takiben 180 gün içerisinde

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
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 gün içerisinde
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/staj Başvurusu/ Burs Başvurusunun 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
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
Şirket faaliyetleri uyarınca, saklanması gereken ticari defterler, ticari defterlerde yer alan kayıtlara dayanak oluşturan 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

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
			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 içeriklerle 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 içeriklerle 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
Sözleşmeden kaynaklı ilişkilerde işlenen kişisel veriler (ör; şirket yetkilisi ad-soyad, imza sirküleri vs.)	Sözleşmenin sona ermesine müteakip 10 yıl	6098 sayılı Türk Borçlar Kanunu	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	5 yıl	213 Sayılı Vergi Usul Kanunu	Saklama süresinin



Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
uyarınca tutulması gereken belgelerle işlenen kişisel veriler			bitimini takiben 180 gün içerisinde
Ziyaretçilerin kişisel verileri	2 yıl	5651 sayılı Kanun (Şirket wi-fi ağına erişim sağlayan ziyaretçiler açısından)	Saklama süresinin bitimini takiben 180 gün içerisinde
CCTV kameraları uyarınca güvenlik amaçlı olarak işlenen kişisel veriler (kamera kayıtları)	90 gün	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanların Kişisel Verilerin yer aldığı ortamlara ilişkin yaptığı erişimlerin Log kayıtları	En az 2 yıl olmak suretiyle İş davalarına konu olabilmesi sebebiyle 10 yıl	5651 sayılı Kanun gereği ve TİB (Telekomünikasyon İletişim Başkanlığı) yönetmelikleri	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket internet ağının kullanılması, İnternet Giriş ve Uzaktan Bağlantı esnasında işlenen Trafik bilgileri (ör;IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri vs)	2 yıl	5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri Bilgilerinden, TTK md.82 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

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
Potansiyel Müşterilere ilişkin veriler	13 ay	Avrupa Birliği/Sektörel Teamül uygulaması	Saklama süresinin bitimini takiben 180 gün içerisinde

## 10. PERİYODİK İMHA SÜRESİ

Mervan Otomotiv Mam. San. Tic. Ltd. Şti. saklama süresi sona eren ve kişisel verinin saklanmasını gerektirecek başka herhangi bir veri işleme amacı mevcut olmayan kişisel verileri, saklama süresinin sona ermesini takiben 180 gün (6 ay) içerisinde anonim hale getirir

## 11. İLGİLİ KİŞİNİN TALEP ETMESİ DURUMUNDA KİŞİSEL VERİLERİN SİLME VE YOK ETME SÜRELERİ

İlgili kişi, Mervan Otomotiv Mam. San. Tic. Ltd. Şti. 'ye 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 politika uyarınca siler, yok 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 durumu 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'üncü 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. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASINDA YAPILACAK GÜNCELLEMELER

Şirket, KVK Kanunu'nda yapılan değişiklikler nedeniyle, KVK Kurumu kararları uyarınca ya da ortaya çıkacak gelişmeler doğrultusunda, Kişisel Verilerin İşlenmesi ve Korunması Politikasında ya da işbu Kişisel Verilerin Saklanması ve İmhası Politikasında değişiklik yapma hakkını saklı tutmaktadır.

İşbu Kişisel Verilerin Saklanması ve İmhası Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır. İşbu politikada yapılacak güncellemeler Şirket tarafından onaylanması üzerine revizyon ve onay tarihi ile birlikte [www.mervanotomotiv.com](http://www.mervanotomotiv.com) adresinde yayımlar.

### 13. YÜRÜRLÜK

İşbu Kişisel Verilerin Saklanması ve İşlenmesi Politikası 13.04.2021 tarihinde Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.

İşbu Kişisel Verilerin Saklanması ve İşlenmesi Politikası ve ileride yapılacak güncellemeler, [www.mervanotomotiv.com](http://www.mervanotomotiv.com) adresinde yayımlanarak erişimine sunulacaktır.

<b>DÖKÜMAN GÜNCELLEME TABLOSU</b>				
<b>Politika Maddesi</b>	<b>Politika Alt Maddesi</b>	<b>Versiyon</b>	<b>Yayın Tarihi</b>	<b>Değişikliğin Tanımı</b>
		1.0	<b>13.04.2021</b>	Kişisel Verilerin Saklanmasına ve İmhasına İlişkin Politika