S.B.S TEKSTİL SANAYİ VE TİCARET A.Ş.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1- Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca yükümlülüklerimizi konu usul ve esasları belirleyerek ve veri sahiplerini, kişisel verilerin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla S.B.S Tekstil Sanayi ve Ticaret A.Ş. ("Şirket") tarafından hazırlanmıştır.

2-Bu Politika kapsamında, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik veya otomatik olmayan yollarla işlenen gerçek kişiler olarak müşteriler, müşteri adayları, çalışan adayları, çalışanlar, şirket hissedarları, şirket yetkilileri, ziyaretçiler, iş ortakları, işbirliği içinde olduğumuz kurumların, alt işverenlerin ve tedarikçilerin çalışanları, hissedarları ve yetkilileri ile üçüncü kişiler bulunmaktadır.

Politika, Şirketimizce yönetilen, tüm kişisel verilerin işlenmesi ve korunmasına yönelik yürütülen faaliyetlerde uygulanmaktadır.

3-İşbu politika şirketimizin internet sitesinde (www.shirtbyshirt.com) yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

4-Bu Politika'nın uygulanmasında kategorisini,

- **İlgili Kişi:** 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 kişileri,
- **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- **Kanun:** 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
- **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 ortamı,
- **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- **Kişisel veri sahibi:** Kişisel verisi işlenen gerçek kişiyi,
- **Kişisel verinin işlenmesi:** 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- **Kişisel veri işleme envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini, kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,
- **Kurul:** Kişisel Verileri Koruma Kurulu'nu,
- **Kurum:** Kişisel Verileri Koruma Kurumu'nu,
- **Özel nitelikli kişisel veri:** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri,
- **Periyodik imha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,
- **Veri Saklama ve İmha Politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları işbu Politikayı,
- **Kişisel Verilerin Korunması,İşlenmesi Ve Gizlilik Politikası:** şirketin internet adresinde yer alan, kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı,

- **Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,
- **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişiyi,
- **Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
- **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Bu Politika'da yer almayan tanımlar için Kanun'daki tanımlar geçerlidir.

5-Şirketin bütün birim yöneticileri, birimlerinde kişisel verilerin işlenmesi, saklanması ve imhası ile ilgili teknik ve idari önlemlerin usulüne uygun uygulanmasına etkin destek verir. Birim yöneticileri bu amaçla; birim çalışanlarının eğitimi ve farkındalıklarının artırılmasını sağlar, işlemleri izleyip denetler, kişisel verilerin hukuka aykırı olarak işlenmesinin ve işlenen verilere hukuka aykırı olarak erişilmesinin önlenmesine, veri güvenliğine yönelik teknik ve idari önlemlerin alınması ve uygulanmasına yardımcı olur.

İlgili kullanıcıların kişisel verilerin korunması hususunda bilgi ve farkındalıkları artırılarak, kişisel verilerle ilgili işleme, saklama ve imha işlemlerinin mevzuata uygun olarak yerine getirilmesine aktif destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımları şöyledir:

- **Genel Müdür** : Veri sorumlusu temsilcisi sıfatıyla, kişisel verilerin korunması ve imhası ile ilgili tüm işlemlerin yapılması ve politikanın uygulanmasından sorumludur.
- **İnsan Kaynakları Yöneticisi** : Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi, görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi, eğitim ve bilgilendirmeden sorumludur.
- **Muhasebe Yöneticisi** : Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi,görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
- **Bilgi Sistemleri Yöneticisi** : Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden, politikanın uygulanmasında gereksinim duyulan teknik çözümlerin belirlenmesi ve uygulanmasından sorumludur.
- **Diğer Birim Yöneticileri** : Kendi birimlerinde politikanın uygulanması ve uygulamanın izlenmesi ve denetlenmesi, görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
- **İlgili Kullanıcı ve Veri İşleyenler** : Veri işleme ve saklanması ile ilgili işlemlerin usul ve yasaya uygun olmasından sorumludur.
- **Özel Yetkili İlgili Kullanıcı** : Prosedür veya ilgili kişinin isteği üzerine silinen kişisel verilerin yok edilinceye kadar korunması, saklanması, ilgili kullanıcılar tarafından erişilmemesinden sorumludur.

6-Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine uygun bir kayıt ortamında tutulmaktadır. Kişisel verilerin saklanması için kullanılan kayıt ortamları aşağıda belirtilmektedir. Öte yandan kişisel verilere nitelikleri gereği burada belirtilen ortamlardan farklı bir ortamda yer verilebilir. Her halde veri sorumlusu şirket, kişisel verileri Kanun'a, Kişisel Verilerin Korunması, İşlenmesi ve Gizlilik Politikası'na ve işbu Kişisel Veri Saklama ve İmha Politikası'na uygun olarak uluslararası veri güvenliği prensipleri çerçevesinde işlemekte ve korumaktadır.

Elektronik Ortamlar; Sunucular, taşınabilir diskler, yazılımlar, bilgi güvenliği cihazları, çalışan bilgisayarları, optik diskler, çıkartılabilir bellekler, yazıcı, tarayıcı ve fotokopi makinesi gibi sair dijital ortamlardır.

Fiziki Ortamlar; Kağıt, manuel veri kayıt sistemleri, yazılı, basılı, görsel ortamlar gibi verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu sair ortamlardır.

Bulut Ortamlar; Şirket nezdinde yer almamakla birlikte, şirketin kullanımında olan ve şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

7- Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nın 12. Maddesindeki ilkeler çerçevesinde, alınmış olan tüm idari ve teknik tedbirler aşağıda belirtilmiştir.

Teknik Tedbirler

Kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- Şirket nezdinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar
- Kişiselverilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanır.
- Kanunun 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli yöntemler ile korunur.

İdari Tedbirler

Kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm şirket çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- Şirket nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

8-Veri sahiplerine ait kişisel veriler, şirket tarafından özellikle ticari faaliyetlerin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması ve ifası, müşteri ilişkilerinin yönetilebilmesi ve Kişisel Verilerin Korunması,İşlenmesi Ve Gizlilik Politikasında yer alan diğer amaçlarla fiziki veya elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır. Şirket nezdinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir. Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

- Kanunlarda açıkça öngörülmesi.
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

9-Şirket tarafından kişisel verilerin silinmesi ve yok edilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır.

KİŞİSEL VERİLERİN SİLİNMESİ

Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması: ilgili evrak üzerindeki kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi yöntemidir.

Yazılımdan Güvenli Olarak Silme: Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel verilerin silinerek bir daha ulaşılamayacak hale getirilmesi yöntemidir.

KİŞİSEL VERİLERİN YOK EDİLMESİ

Fiziksel Yok Etme: Kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kağıt ortamında bulunan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir. Kişisel veri barındıran optik ve manyetik medya ise eritilme, yakılma veya toz haline getirilme gibi fiziksel olarak yok edilir.

De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir.

Üzerine yazma: Özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini ortadan kaldıran yok etme yöntemidir.

KİŞİSEL VERİLERİN ANONİMLEŞTİRİLMESİ

Değişkenleri çıkarma: İlgili kişiye ait toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden yüksek dereceli betimleyici olanların çıkartılarak anonim hale getirilmesi yöntemidir.

Bölgesel gizleme: Tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır**.** İstisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.

Genelleştirme: Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.

Alt ve Üst Sınır Kodlama: Önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmesi yöntemidir.

Mikro birleştirme: Tüm veriler ilk olarak anlamlı bir sıraya dizilerekgruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanır.

Veri karma ve bozma: Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

10-Saklama ve İmha Süreleri

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren 10 yıl müddetle muhafaza edilir.	Saklama süresinin bitimini takiben 180 gün içerisinde
İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren 10 yıl müddetle saklanır	Saklama süresinin bitimini takiben 180 gün içerisinde

İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin devamında ve hitamından itibaren 10 yıl müddetle saklanır	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İşilişkisinin sona ermesine müteakip 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel Finansman Süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
İş Ortağı/Çözüm Ortağı/Danışman ile şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, İş Ortağı/ÇözümOrtağı/Danışman çalışanı verileri	Şirket ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Fiziki mekanlara girişte alınan Ziyaretçi'ye ait ad, soyad, araç plakası ile kamera kayıtları,	2 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Stajyer'e ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10 yıl müddetle muhafaza edilir.	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, ürün/hizmet tercihleri, işlem geçmişi,	Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Potansiyel Müşteri ile şirket arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler,	2 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
İşbirliği içinde olunan kurum,firmalar ve müşteriler ile şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, şirketin işbirliği içinde olduğu kurum,firma, müşteri çalışanı verileri	Şirket ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Kurumsal İletişim Faaliyetlerinin Planlanması ve İcrası	İş ilişkisinin sona ermesine müteakip 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Bir Sözleşmenin Kurulması veya İfası İçin İşlenmesi Gerekli Olan veya Bu Kapsamda İşlenen Diğer Veriler	Şirket ile iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Kaza Raporlama	10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Doküman hazırlanması	10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde
Eğitim kayıtlarının dosyalanması	10 yıl süre ile saklanır.	Saklama süresinin bitimini takiben 180 gün içerisinde

11-Kanun kapsamında kişisel verilerin saklanması için herhangi bir süre belirlenmemiş olmakla birlikte, genel ilkeler uyarınca kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi esastır. Veri Sorumlusu Şirket, söz konusu ilkeye uygun bir şekilde saklama süreleri tespit etmek adına, her bir veri işleme süreci ile ilgili olarak yürürlükte bulunan mevzuatı ve sürecin amacını esas alarak bir değerlendirme yapmaktadır. Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir. Bu doğrultuda asgari olarak yasal yükümlülüklerinin gerektirdiği süre ve ilgili Kanuna konu zamanaşımı süreleri dolana kadar kişisel veriler saklanmaktadır.

Kişisel veriler, Veri Sorumlusu ile aranızda doğabilecek herhangi bir uyuşmazlık durumunda, uyuşmazlık kapsamında gerekli savunmaların gerçekleştirilebilmesi amacıyla saklanabilecektir. Bahsi geçen sürelerin sona ermesi durumu da dahil olmak üzere herhangi bir süreç kapsamında ilgili kişisel verinin işleme amacının ortadan kalkması ile birlikte kişisel veriler Kanuna uygun bir şekilde anonimleştirilmekte, silinmekte veya yok edilmektedir.

12- Saklama süresi sona eren veya saklama amacı ortadan kalkan kişisel veriler işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemlerle altı ayda bir imha edilmek suretiyle silinir, yok edilir veya anonim hale getirilir. Periyodik imha işlemi her yılın Ocak ve Temmuz aylarında ayrıca gerçekleştirilir.

13-Şirketimiz, KVK Kanunu'ndaki yükümlülükleri yerine getirmek ve işbu Politikada belirtilen hususların uygulanmasına yönelik olarak Şirket içerisinde gerekli görevlendirmeleri yapmakta ve buna uygun olarak prosedürleri oluşturmaktadır.

14-Şirket faaliyetleri ve işlenen kişisel veri gruplarında olabilecek değişiklikler, yasal mevzuatta yapılacak değişikler ve Kişisel Verileri Koruma Kurulu ilke kararları takip edilerek, ortaya çıkan ihtiyaca göre işbu politika gözden geçirilir ve gerekli olan bölümler güncellenir, değiştirilir veya yeniden oluşturulur