

**KİŞİSEL VERİ SAKLAMA VE
İMHA POLİTİKASI**

1. HEDEF VE KAPSAM

Tedarik Zinciri Yönetimi Derneği (Bundan böyle “**Veri Sorumlusu**” olarak anılacaktır), ticari varlık ve başarılarını desteklediği etik değerleri gereği hukuki düzenlemelere riayet edilmesi konusunda yüksek hassasiyet sahibi olup, kişisel verilerin korunmasına ilişkin mevzuata uyum çerçevesinde gerekli her türlü yapılanmayı tesis etmektedir.

Kişisel Veri Saklama ve İmha Politikası vasıtasıyla, Veri Sorumlusu tarafından işlenen kişisel verileri şirket bünyesinde bulundurma ve imha etme süreçlerinde benimsenen ilke ve esaslar düzenlenmektedir.

Veri Sorumlusu tarafından hukuka uygun şekilde işlenen kişisel verilerin, işlenmesini gerektiren sebeplerin ortadan kalkması ya da veri sahibinin imhaya ilişkin talepte bulunması üzerine işbu Politika hükümleri uygulanacaktır.

2. DAYANAK

Kişisel Veri İmha Politikası; KVK Kanunu ve [Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik](#) gereği yayımlanmış olup; [Kişisel Verilerin Korunması ve İşlenmesi Politikası](#) ve Kişisel Verileri Koruma Kurumu tarafından yayımlanan yayın ve rehberlere sırayet ederek hazırlanmıştır.

3. VERİ SORUMLUSU

Tüzel kişiliği altında işlenen kişisel verilerin işleme amaç ve vasıtalarını belirleyen ve veri işleme faaliyetinden sorumlu olan Veri Sorumlusu; KVK Kanunu gereği veri sorumlusudur.

İşbu politika gereği; Veri Sorumlusu bünyesinde işlenen kişisel verilerin imha süreçlerinde Veri Güvenliği Kurulu yetkilidir.

4. TANIMLAR

Veri Sorumlusu Kişisel Veri Saklama ve İmha Politikası ve mevzuatta yer alan önemli tanımlar anlamlarıyla birlikte aşağıdaki tabloda yer almaktadır:

Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Özel Nitelikteki Kişisel Veri	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler
Veri Sahibi	Kişisel verisi işlenen belirli ya da belirlenebilir gerçek kişi (İlgili kişi)
Kişisel Verilerin İmhası	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kişisel Verilerin İşlenmesi	Kişisel verilerin 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 işlem
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzelkişi
Periyodik İmha	Kişisel veri işleme ve saklama süresi dolduğunda Veri Sorumlusu tarafından, tekrar eden aralıklarla ve Resen gerçekleştirilecek olan imha işlemi
KVK Kanunu (Kanun)	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete’de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu
Veri Güvenliği Kurulu	Veri Sorumlusu tarafından, kişisel verilerin korunması mevzuatına uygunluğun sağlanması, muhafazası ve sürdürülmesi kapsamında Şirket bünyesinde gerekli koordinasyonu sağlayacak olan Kurul
KVK Kurumu (Kurum)	Kişisel Verileri Koruma Kurumu
Veri İhlali	Kişisel verilerin korunması hukukunda; işlenen kişisel verilerin kanuni olmayan yollarla üçüncü şahısların eline geçmesi

5. KİŞİSEL VERİLERİN SAKLANMASI

Veri Sorumlusu nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur. Veri Sorumlusu; kişisel verilerin, güvenli şekilde saklanması ve hukuka aykırı müdahalelere maruz kalmaması adına gerekli idari ve teknik tedbirleri alır. Veri güvenliğine ilişkin alınan tedbirler ve veri saklama gerekçeleri hususlarında Kişisel Verilerin Korunması ve İşlenmesi Politikası'na riayet edilir.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibarıyla aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları farklı nitelik ya da Veri Sorumlusu'nun hukuki yükümlülükleri nedeniyle aşağıda gösterilen ortamlardan farklı bir ortamda tutulabilir.

Fiziki Ortamlar	Kağıt ve benzeri fiziki yollarla saklanan kişisel veriler
Elektronik Ortamlar	Veri Sorumlusu bünyesinde yer alan ve yalnızca Veri Sorumlusu'nun erişim yetkisini haiz olduğu sunucu ve harici disklerde saklanan kişisel veriler
Bulut Ortamlar	Kriprografik yöntemler kullanılarak şifrelenmiş internet tabanlı sistemlerden yararlanılarak saklanan kişisel veriler

6. KİŞİSEL VERİLERİN İMHA EDİLMESİ

Kişisel verilerin imha edilmesi; işleme amacını yitiren ya da veri sahibinin talepte bulunduğu kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi süreçlerini ifade eder. Kişisel verinin varlığı sözleşmesel, ticari, hukuki, idari işlemler gereğince doğması muhtemele hak taleplerine ilişkin ise söz konusu işleme ilişkin zamanaşımı süresince veriler muhafaza edilir.

Veri Sorumlusu bünyesinde işlenen kişisel veriler; İlgili kişinin talebi halinde ya da KVK Kanunu'nun 5'nci ve 6'ncı maddelerinde ve Veri Sorumlusu Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda sayılan veri işleme nedenlerinin ortadan kalkması halinde resen işbu Politika uyarınca silinir, yok edilir veya anonim hale getirilir.

Veri Güvenliği Kurulu; Veri Sorumlusu tarafından işlenmekte olan tüm kişisel veriler için 6 aylık zaman aralıkları ile periyodik imha işlemi gerçekleştirir.

7. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Silinen verilere, veri sorumlusu haricinde bulunan ilgili kullanıcılar tarafından erişilemez.

Bu konuda talep ve şirket politikası arasında bir çelişki doğması halinde çelişkinin giderilmesi amacı ile Kişisel Verileri Korunma Kurumu'na yazılı başvuru yapılır ve ilke kararı doğrultusunda işlem yapılır.

Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcılar tespit edilir ve kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespiti yapılarak akabinde ilgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılmasına ilişkin işlemler gerçekleştirilir.

7.1. SİLME TEKNİKLERİ

7.1.1. KARARTMA

Kağıt ortamında bulunan ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilerek, aksi halde mürekkep kullanılarak kullanıcılar tarafından görünmez kılınması tekniğidir.

7.1.2. DİJİTAL ORTAMDAN GÜVENLİ ŞEKİLDE SİLME

Merkezi sunucularda ve bulutta yer alan kişisel veriler, işletim sistemindeki silme komutu ile güvenli şekilde silinir.

8. KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi, silinmesinden farklı olarak imha işlemi sonrasında veri sorumlusunun da söz konusu verilere erişememesi anlamına gelir.

8.1. YOK ETME TEKNİKLERİ

8.1.1. DE-MANYETİZE

Manyetik medya, de-manyetize etme özellikli bir cihazdan geçirilerek verilerin okunamaz biçimde bozulur. De-manyetize özellikli cihaz ihtiyaç halinde Veri Sorumlusu tarafından temin edilir.

8.1.2. FİZİKSEL YOK ETME

Optik medya ve manyetik medya eritilerek, yakılarak veya toz haline getirilerek fiziksel olarak yok edilir.

8.1.3. ÜZERİNE YAZMA

Manyetik medya yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilir. Gerek halinde şirket tarafından bu amaçla yazılım temin edilir.

8.1.4. DİJİTAL ORTAMDAN GÜVENLİ ŞEKİLDE YOK ETME

Merkezi sunucularda yer alan kişisel veriler, işletim sistemindeki yok etme komutu ile bir daha geri döndürülemeyecek şekilde yok edilir.

9. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi; kişisel verinin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemidir. Veri Sorumlusu; kişisel verilerin anonim hale getirilmesi ile alakalı her türlü güvenlik önlemini alır.

9.1. ANONİM HALE GETİRME TEKNİKLERİ

Kişisel verilerin anonim hale getirilmesinde; gruplama, maskeleyme, türetme, genelleştirme, rastgele hale getirme gibi teknikler bulunmaktadır. Veri Sorumlusu; anonimleştirme yöntemini seçerken, kişisel verinin niteliği ve büyüklüğü, kişisel verinin fiziki ortamlarda bulunma yapısı ve çeşitliliği, veriden sağlanmak istenen fayda / işleme amacı, verinin işlenme sıklığı, kişisel verinin aktarılacağı 3. şahısların güvenilirliği, anonimleştirme için gereken çabanın anlamlı olması, kişisel verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı, verinin

dağıtıklık/merkezilik oranı, kullanıcıların ilgili veriye erişim yetki kontrolü ve anonimliği bozacak bir saldırı ihtimallerini dikkate alır.

Veri Sorumlusu tarafından işlenen kişisel veri kategorilerinin saklama sebep ve süreleri aşağıdaki tabloda belirtilmiştir. Saklama süresi dolan her veri, takip eden ilk periyodik imha süresinde imha edilir. Kanuni ve sözleşmesel yükümlülüklerin ifası kapsamında gerektiği takdirde bu süre değişiklik gösterebilecek olup, ilgili yükümlülüğün ortadan kalması üzerine takip eden ilk periyodik imha süresinde imha edilir.

Veri Kategorisi	Saklama Süresi	Saklama Sebebi
Özlük Verileri	5510 Sayılı Kanuna göre belge saklama süresi, belgenin ilgili olduğu yılı takip eden yılbaşından başlamak üzere 10 yıldır .	Çalışanlar için iş akdi ve mevzuattan doğan yükümlülüklerin yerine getirilmesi
Mesleki Deneyim	Çalışan adaylarının özgeçmiş bilgileri 3 ay süreyle saklanır.	Çalışan adaylarının başvuru süreçlerinin yürütülmesi
Kimlik ve İletişim Verileri	Müşteri ve müşteri adayına ilişkin alınan iletişim bilgileri 10 yıl süreyle saklanır.	İletişim faaliyetlerinin yürütülmesi
Hukuki İşlem	İşlem tarihinden itibaren 10 yıl süreyle saklanır.	Yetkili yargı / idari kurum ve merciler tarafından iletilen taleplerin cevaplandırılması
Müşteri İşlem	TBK. İlgili hükümler doğrultusunda 10 yıl süreyle saklanır.	Mal / hizmet satın alım ve satış süreçlerinin yürütülmesi ve müşteri memnuniyetinin sağlanması
Finans ve Muhasebe Verileri	TTK. md. 82'ye göre 10 yıl süreyle saklanır.	Finans ve muhasebe işlerinin yürütülmesi
İşlem/Pazarlama Verileri	Elde edilmesinden itibaren 10 yıl süreyle saklanır.	Pazarlama faaliyet ve çalışmalarının yürütülmesi
Özel Nitelikli Kişisel Bilgi	İş sağlığı ve güvenliği hükümlerine göre 10 yıl süreyle saklanır.	İş Sağlığı / Güvenliği ve Hukuk işlerinin takibinin yürütülmesi ve İş sağlığı ve güvenliği yükümlülüklerinin sağlanması
Fiziksel Mekan Güvenliği	Güvenlik kamerası kayıtları 3 aylık süre boyunca saklanır.	Fiziksel mekan güvenliğinin temini

İşlem Güvenliği	10 yıl süreyle saklanır.	Bilgi güvenliği süreçlerinin yürütülmesi
Diğer	10 yıl süre ile saklanır	Şirket faaliyetlerinin sürekliliği
Görsel/İşitsel Bilgi	Kaydın oluşturulmasından itibaren 6 ay saklanır.	Fiziksel mekan güvenliğinin ile birlikte müşteri memnuniyeti temini

10. VERİ SAHİBİ İMHA TALEPLERİ

Veri sahibi tarafından imha talebinin Veri Sorumlusu'na iletilmesi halinde; durum 24 saat içerisinde Veri Güvenliği Kurulu'na bildirilir. Talebin cevaplandırılması süreçlerinde [Veri Sorumlusu Veri Sahibi İlişkileri Kılavuzu](#)'na riayet edilir.

Veri Sorumlusu'na iletilen veri sahibi başvurusunun bir veri ihlali ihtimaline yönelik bulgular barındırması halinde [Veri Sorumlusu Veri İhlali Prosedürü](#) uygulamaya konulur. İhlal ihtimali derhal ve en geç 24 saat içerisinde Veri Güvenliği Kurulu'na bildirilir.

11. İHLAL ve YAPTIRIMLAR

Veri sorumlusu tarafından yayınlanmış olan kişisel verilere ilişkin politika ve prosedürlerin çalışanlar tarafından ihlal edilmesi halinde; İş Sözleşmesi ve [4857 sayılı İş Kanunu](#) gereğince çalışanın savunması alınır ve fiile uygun disiplin tedbiri tesis edilir. Fiilin aynı zamanda [5237 sayılı Türk Ceza Kanunu](#) veya sair kanunlarca suç teşkil etmesi halinde gerekli adli mercilere bildirim yapılır.

12. REVİZYON

İşbu Politika, Veri Güvenliği Kurulu tarafından onaylandığı andan itibaren yürürlüğe girer. İşbu Politika'nın yürürlükten kaldırılması hususu hariç olmak üzere Politika içerisinde yapılacak değişiklikler ve ne şekilde yürürlüğe konacağı konusunda yine Veri Güvenliği Kurulu yetkilidir.

Veri Sorumlusu Kişisel Veri Saklama ve İmha Politikası her halükarda yılda bir kez gözden geçirilir, gerekli değişiklikler varsa, Veri Güvenliği Kurulu onayına sunularak güncellenir. Başta KVK Kanunu olmak üzere yürürlükteki mevzuat ile işbu Politikada yer verilen düzenlemelerin gelişmesi halinde mevzuat hükümleri uygulanır.

Veri Sorumlusu, idari otorite olan KVK Kurumu tarafından yapılacak olan yasal düzenlemelere paralel olarak Veri Sorumlusu Kişisel Veri Saklama ve İmha Politikasına değişiklik yapma hakkını saklı tutar. İşbu prosedür veya mevzuatta oluşabilecek revizyonlar tarih ve konu belirtilerek prosedüre

eklenecek, gerekli duyurular yapıldıktan sonra prosedürün ayrılmaz bir parçası olarak kabul edilecektir.

EKİ :

i) Kişisel Veri Saklama Amaçları (EK-1)

ii) Kişisel Veri Sahipleri (EK-2)

iii) Kişisel Veri Kategorileri (EK-3)

EK-1 Kişisel Veri Saklama Amaçları

Birincil Amaç	İkincil Amaç
Şirket'in insan kaynakları politikaları ve süreçlerinin planlanması ve yürütülmesi	<ul style="list-style-type: none">i. Şirket tarafından yürütülen faaliyetler çerçevesinde hizmet sunumu amacıyla personel temin süreçlerinin yürütülmesiii. Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesiiii. Çalışanların performans değerlendirme süreçlerinin yönetilmesiiv. Ücret politikasının yürütülmesiv. Yetenek, kariyer gelişimi faaliyetlerinin yürütülmesivi. Çalışan talep ve şikayet yönetimivii. Şirket çalışanlarının memnuniyet ve bağlılığının artırılmasına yönelik süreçlerin planlanması ve yönetilmesiviii. Şirket içerisinde personel ve yöneticilerin atama ve terfi süreçlerinin yönetimine destek olunması
Şirket tarafından yürütülen ticari faaliyetlerin gerçekleştirilmesi için ilgili iş birimi tarafından gerekli çalışmaların yapılması ve buna bağlı iş süreçlerinin yürütülmesi	<ul style="list-style-type: none">i. Finans ve/veya muhasebe işlerinin takibiii. Yönetim faaliyetlerinin yürütülmesiiii. İş faaliyetlerinin satın alım süreçleri ile birlikte satış sonrası destek hizmetlerinin yürütülmesi,iv. İş faaliyetlerinin etkinlik/verimlilik ve/veya yerindelik analizlerinin gerçekleştirilmesi faaliyetlerinin planlanması ve/veya icrası

<p>Şirket'in hukuki, teknik ve ticari-iş güvenliğinin temini</p>	<ol style="list-style-type: none">i. Hukuk işlerinin takibiii. Şirket faaliyetlerinin şirket prosedürleri ve/veya ilgili mevzuata uygun olarak yürütülmesinin temini ve denetimi için gerekli operasyonel faaliyetlerinin planlanması ve yürütülmesiiii. İş sürekliliğinin sağlanması ve iş faaliyetlerinin yürütülmesiiv. Şirket kaynaklarının güvenliğinin teminiv. Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesivi. Verilerin doğru ve güncel tutulmasıvii. Müşteri/Ziyaretçi Kayıtlarının Oluşturulması ve Takibi
------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

EK-2 Kişisel Veri Sahipleri

Kişisel veri sahibi kategorisi	Açıklama
Stajyer	Şirket tarafından yürütülen etkinlik, çalışan memnuniyeti, insan kaynakları, denetim, bilgi teknolojileri güvenliği ve altyapısının sağlanması, hukuki uyum vb faaliyetler çerçevesinde kişisel verileri işlenen Şirket stajyerleri
Çalışan Adayı	Şirket'e herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini Şirket'in incelemesine göndermiş olan gerçek kişiler.
Çalışan	Şirket tarafından yürütülen etkinlik, çalışan memnuniyeti, insan kaynakları, denetim, bilgi teknolojileri güvenliği ve altyapısının sağlanması, hukuki uyum vb faaliyetler çerçevesinde kişisel verileri işlenen Şirket çalışanları
Tedarikçi Çalışanı/Yetkilisi	Şirket'in ticari faaliyetlerini yürütürken Şirket emir ve talimatlarına uygun olarak sözleşmesel ilişki kapsamında hizmet sunan taraf çalışanı veya yetkilisi olan gerçek kişiler.
Ürün/Hizmet Alan Kişi	Şirket ile herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirket iş birimlerinin yürüttüğü faaliyet, hizmet ve operasyonlar kapsamında kişisel verileri elde edilen gerçek veya tüzel kişiler
Ziyaretçi	Şirket'in sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerini ziyaret eden gerçek kişiler

EK-3 Kişisel Veri Kategorileri

KİŞİSEL VERİ KATEGORİZASYONU	KİŞİSEL VERİ KATEGORİZASYONU AÇIKLAMA
Kimlik Bilgisi	Kişinin kimliğine dair bilgilerin bulunduğu veriler olup ad-soyad, T.C. kimlik numarası, uyruk bilgisi, doğum yeri, doğum tarihi, cinsiyet vb. bilgiler ile ehliyet, mesleki kimlik, nüfus cüzdanı ve pasaport gibi belgeler
İletişim Bilgisi	Telefon numarası, adres, e-mail adresi, faks numarası vb. bilgiler
Özlük Bilgisi	Çalışanın bordro ve özgeçmiş bilgileri ile disiplin soruşturması, işe giriş belgesi kayıtları, performans değerlendirme raporları vb. belgeler
Müşteri İşlem/Pazarlama Bilgisi	Şirket tarafından yürütülen faaliyetler çerçevesinde, sunulan hizmetlerle ilgili hizmet kalitesini artırmak, müşteri memnuniyetini korumak amacıyla işlenen anket bilgisi, beyan bilgisi, çağrı merkezi kayıtları, cookie kayıtları gibi veriler
Fiziksel Mekan Güvenlik Bilgisi	Fiziksel mekana girişte, fiziksel mekanın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler; kamera kayıtlar ve güvenlik noktasında alınan kayıtlar vb.
Finansal ve Muhasebe Bilgi	Kişisel veri sahibi ile kurulmuş olan hukuki ilişkinin tipine göre yaratılan her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler ile banka hesap numarası, IBAN numarası gibi veriler

Görsel/İşitsel Bilgi	Fotoğraf ve kamera kayıtları (Fiziksel Mekan Güvenlik Bilgisi kapsamında giren kayıtlar hariç) ve ses kayıtları
Özel Nitelikli Kişisel Bilgi	Kişilerin sendika üyeliği, sağlığı ve ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili verileri
Hukuki İşlem Bilgisi	Hukuki alacak ve hakların tespiti, takibi ve borçların ifası ile kanuni yükümlülükler ile birlikte Şirket politikalarına uyum kapsamında işlenen kişisel veriler
Diğer	Şirket faaliyetlerinin sürekliliği kapsamında işlenen kişisel veriler