1. KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASININ AMACI

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a (Kanun) dayalı olarak çıkarılmış olan ve 30224 sayılı Resmî Gazete'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (Yönetmelik) gereği kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin yerine getirilmesi için Şirket'imiz tarafından uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

2. KAPSAM

Bu Kişisel Veri Saklama ve İmha Politikası (Politika) Kanun ile tanımlanan Kişisel Verileri ve Özel Nitelikli Kişisel Verileri, tüm Şirket çalışanlarını, temsilcilerini, danışmanlarını, tüm iştiraklerini, dış hizmet sağlayıcılarını, Şirketin hukuki ilişkiye girdiği tüm gerçek ve tüzel kişileri kapsamaktadır.
Politikada aksi belirtilmedikçe Kişisel Veriler ve Özel Nitelikli Kişisel Veriler "Kişisel Veriler" olarak anılacaktır.
Politika Şirket'in Kişisel Veriler üzerinde uygulayacağı saklama faaliyetleri hakkında bilgi verecek olup, imha faaliyetlerini de kapsayacak ve her türlü imha eylemi sürecinde uygulanacaktır.
Politika kapsamında saklama ve imha sorumluları ve saklama ve imha ile ilgili süreler Politika'nın sonundaki ek tablolarda verilmiştir.
Bu Politika Şirket'in uyguladığı diğer Kişisel Verileri Koruma ve Gizlilik politikalarıyla birlikte uygulanır ve Şirket politikaları birbirlerinin tamamlayıcılarıdır. Söz konusu politikaları aşağıdaki adreslerde bulabilirsiniz:

KVKK Veri İşleme Politikası :
http://www.metalyapi.com/Media/Default/Pdf/kvkk/Kisisel_Verilerin_Korunmasi_Kanunu_Proseduru_AS.pdf

3. TANIMLAR VE KISALTMALAR

3.1. Alenileştirme: İlgili kişinin kendisi tarafından herhangi bir şekilde kamuya açıklanmış olan veri.
3.2. Bulut Ortamı: Şirket bünyesinde yer almamakla birlikte, Şirket'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlar.
3.3. Güvenlik Duvarı: Birçok farklı filtreleme özelliği ile ağın gelen ve giden paketler bazında trafiğini kontrol altında tutar ve güvenliğini sağlar.
3.4. İlgili Kişi: Kişisel Verisi işlenen gerçek kişi.
3.5. İlgili Kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişi.
3.6. Karartma: Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemler.
3.7. Kanun: 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun.
3.8. Kayıt Ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
3.9. Kişisel Veriler: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
3.10. Kişisel Verilerin İşlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
3.11. Maskeleme: Kişisel Verinin temel belirleyici bilgisinin veri içerisinden çıkartılarak Kişisel Verinin anonim hale getirilmesi yöntemi.
3.12. Matbu Ortamlar: Verilerin kâğıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
3.13. Özel Nitelikli Kişisel Veriler: 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.

ELEKTRONİK NÜSHADIR. BASILI HALİ KONTROLSÜZ KOPYADIR.

3.14. Politika: Bu Kişisel Veri Saklama ve İmha Politikası
3.15.Toplulaştırma: Birçok verinin toplulaştırılması ve kişisel verilerin bir kişiye ilişkilendirilemeyecek hale getirilmesi yöntemi.
3.16.Veri Karma: Kişisel Veri seti içindeki değerlerin karıştırılarak değerler ve kişiler arasındaki bağın kopartılması yöntemi.
3.17.Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
3.18.Veri Türetme: Kişisel Verilerin içeriğinden daha genel bir içerik oluşturulması ve kişisel verilerin herhangi bir kişiyle ilişkilendirilemeyecek hala getirilmesi yöntemi.
3.19.Yerel Optik, Dijital ya da Manyetik Ortam: Şirket bünyesinde yer alan sabit ya da taşınabilir diskler, optik diskler, SSD'ler, gibi sair ortamlardır.
3.20.Yönetmelik: 30224 sayılı Resmi Gazete'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

4. KAYIT ORTAMLARI

Şirket, kişisel veri barındıran aşağıda sayılmış olan kayıt ortamlarını ve bunlara ek olarak kullanılabilecek her türlü kayıt ortamını bu politikanın kapsamına alacağını beyan ve taahhüt eder. Sayılanlarla sınırlı olmamak üzere, mevcut temel kayıt ortamları şunlardır:

• Şirket adına kayıtlı bilgisayar ve sunucular,
• NAS

5. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN DURUMLAR

5.1. Kişisel Verilerin Saklanmasını Gerektiren Durumlar

Kişisel Veriler, mevzuat uyarınca ve ilgili Şirket Kişisel Veri Politikalarında belirtilen amaç ve nedenlerle saklanacaktır.

5.2. Kişisel Verilerin İmhasını Gerektiren Durumlar

Mevzuat genelindeki özel durumlar, yetkili kurumların talimatları ve istisnalar hariç olmak üzere, Kişisel Veriler ilgili kişinin talebi üzerine ve/veya Kanun'un 5. ve 6. maddelerinde sayılan veri işleme nedenlerin ortadan kalkması nedeniyle resen işbu Politika uyarınca silinir. Bu sayılan nedenler şunlardır:

• 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.

6. KİŞİSEL VERİLERİN GÜVENLİ SAKLANMASI VE MEVZUATA UYGUNLUK İÇİN ALINMIŞ TEDBİRLER

Şirket, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişimi önlemek ve verilerin saklanması için uygun güvenlik önlemlerini almak için gerekli teknik ve idari tedbirleri almakta ve gerekli denetimleri yapmaktadır.
Kişisel Veriler sadece Kanun'da ve diğer mevzuatta belirlenmiş usul ve esasların kapsamında işlenmektedir. Şirket, Kişisel Verileri işlerken aşağıda belirtilen ilkelere uymaktadır:

• Kişisel Verileri ilgili Kişisel Veri politikaları, Kanun ve ilgili mevzuat ile belirlenen sınırlar çerçevesinde kendisinden beklenen işin gerçekleştirilmesinden öte hiçbir amaçla kullanmama.

•Kişisel Verileri hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel olarak, belirli, açık ve meşru amaçlar için, işlendikleri amaçla bağlantılı, sınırlı, ölçülü ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek suretiyle işleme.
• Kanun uyarınca İlgili Kişi tarafından iletilen talepleri derhal yerine getirme.
Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek için Şirket,
• Teknik ve hukuki alanlarda uzman personeller istihdam etmekte,
• Alınan teknik tedbirler periyodik olarak denetlenmekte ve ilgilisine raporlanmakta,
• Kişisel Verilerin hukuka uygun işlenmesi için çalışanlar nezdinde farkındalık yaratılmakta ve gerekli idari ve teknik tedbirler Şirket içi politikalar ve eğitimlerle hayata geçirilmektedir.
Kişisel Verilere hukuka aykırı olarak erişimi engellemek için Şirket,
• Teknolojideki gelişmelere uygun önlemler almakta ve alınan önlemleri teknik ve hukuki açılardan güncel tutmakta,
• Erişim yetkileri sınırlandırmakta ve yetkiler düzenli olarak gözden geçirmekte,
• Alınan tüm önlemler periyodik olarak denetlenmekte, yetkili kişilere raporlanmakta ve risk teşkil eden hususlar açısından teknolojinin sunduğu en ileri tekniklerle çözümler üretmekte,
• Virüs koruma sistemleri ve güvenlik duvarları içeren yazılımlar kullanmakta,
• Teknik konularda uzman personel istihdam etmekte ve düzenli olarak kullanılan uygulamalar güvenlik açıklarının tespiti ve kapatılması için test edilmekte,
• Çalışanları, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacakları ve işleme amacı dışında kullanamayacakları ve bu yükümlülüklerin görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda çalışanlardan gerekli taahhütler almaktadır.

Kişisel Verilerin saklanması için uygun önlemleri almak amacıyla Şirket,

• En üst düzeyde güvenliği sağlayan, teknolojik gelişmelere uygun sistemleri kullanmakta,
• Teknik konularda uzman personel istihdam etmekte,
• Saklama alanlarına yönelik teknik güvenlik önlemleri almakta ve alınan tüm önlemler periyodik olarak denetlenmekte, yetkili kişilere raporlanmakta ve risk teşkil eden hususlar açısından teknolojinin sunduğu en ileri tekniklerle çözümler üretmekte,
• Kişisel Verilerin hukuka uygun bir biçimde saklanması için arızalara karşı emniyetli ve çok katmanlı yedekleme sistemleri kullanmakta,
• Saklama alanlarına tüm erişimler kaydedilmekte ve uygunsuz erişimleri ya da erişim denemelerini anlık olarak ilgilere iletmekte,
• Çalışanları saklanan Kişisel Verilerin güvenliğinin nasıl sağlanabileceği hakkında eğitmektedir.
Ayrıca, Şirket tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.

7. KİŞİSEL VERİLERİN İMHA USUL VE İLKELERİ

Kişisel verilerin imhası üç farklı şekilde gerçekleştirebilir. Bunlar, Kişisel Verilerin silinmeleri, yok edilmeleri ya da anonim hale getirilmeleridir.

7.1. Kişisel Verilerin Silinmeleri:

Kişisel Verilerin silinmeleri, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmeleridir. Mevzuat hükümlerine uygun bir şekilde işlenmiş olan Kişisel Verilerin, işlenme nedenleri ortadan kalktıktan sonra, Şirket resen ya da ilgili kişinin talebi üzerine Kişisel Verileri siler. Bulut ortamında ya da yerel optik, manyetik ya da dijital ortamlarda tutulan Kişisel Veriler bir daha kurtarılamayacak şekilde dijital komutlarla silinirler. Bu şekilde silinen verilere ilgili kullanıcılar bir daha ulaşamazlar. Matbu ortamlarda bulunan Kişisel Veriler ise karartma yöntemi ile silinirler. Karatma işlemi, evrak üzerindeki kişisel verilerin karartılmaları ile yapılır.

7.2. Kişisel Verilerin Yok Edilmeleri:

Kişisel Verilerin yok edilmeleri, kişisel verilerin hiçbir kişi tarafından erişilemez, geri getirilemez ve tekrar kullanılamaz hala getirilmesidir. Şirket, mevzuat hükümlerine uygun şekilde işlenmiş olan Kişisel Verilerin işlenme nedenleri ortadan kalktıktan sonra resen ya da ilgili kişinin talebi üzerine Kişisel Verilerin bulunduğu kayıt ortamlarını sonradan kullanılamayacak bir şekilde fiziksel olarak yok eder.
Matbu ortamda bulunan belgeler evrak imha makineleriyle tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel optik, manyetik ya da dijital ortamlarda saklanan Kişisel Veriler açısından, optik, manyetik ya da dijital medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

7.3. Kişisel Verilen Anonim Hale Getirilmeleri:

Kişisel Verilerin anonim hale getirilmeleri, Kişisel Verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
Kişisel Verilerin anonim hale getirilmeleri için şirket maskeleme, toplulaştırma, veri türetme ve veri karma yöntemlerini kullanır.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel Verilerin yasal saklanma süreleri aşağıdaki tabloda olduğu gibidir:

KİŞİSEL VERİ KATEGORİSİ	AZAMİ SAKLAMA SÜRELERİ
Müşteri Bilgileri	Türk Ticaret Kanunu 82. madde uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesi, esas bilgiler olarak anılan kanun maddesi gereği 10 yıl süre ile, bunun dışındaki Müşteri Bilgileri ise işlendikleri amaç için gerekli olan süre kadar saklanır.
Özlük Bilgileri	Hizmet akdi sona erdikten sonra 10 yıl. Çalışanların Kişisel Sağlık Dosyaları; İş Sağlığı ve Güvenliği mevzuatına göre kişisel sağlık dosyalarının 15 yıl saklanması gerekmektedir.
Çalışan Adayı Bilgileri	1 yıl süre ile saklanır.
Ziyaretçi Bilgileri	2 yıl süre ile saklanır.
İş Ortağı ve Danışman Bilgileri	Şirket ile olan ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu 146. maddesi uyarınca 10 yıl süre ile saklanır.
Firmalar Tarafından Şirket ile Paylaşılan Bilgiler	Şirket ile olan ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu 146. maddesi uyarınca 10 yıl süre ile saklanır.
Potansiyel Müşteri Bilgileri	2 yıl saklanır.

Mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süresi vb. olarak daha uzun bir süre belirlenmiş ise, yukardaki tablodaki azami süreler yerine, herhangi bir hak kaybı olmasını önlemek ve hukuka uygunluk için mevzuatta geçen süre kullanılacaktır. Yönetmeliğin 11'inci maddesi gereğince Şirket periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket'te her yıl Nisan ve Ekim aylarında periyodik imha işlemi gerçekleştirilir.
Eğer ilgili kişi, Kanun'un 13. maddesine uygun olarak şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ederse, kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, anonim hale getirir ya da yok eder. Şirketin talebi almış sayılması için ilgili kişinin talebini şirket politikalarına uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep şirket tarafından Kanun'un 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Hazırlayan	Kontrol Eden	Onaylayan
Eda Demirci	Suna Doğan	Oktay Usta
İK Uzmanı	İK Direktörü	Kalite Yönetim Müdürü

ELEKTRONİK NÜSHADIR. BASILI HALİ KONTROLSÜZ KOPYADIR.

EK 1 – TABLOLAR

TABLO 1 – KİŞİSEL VERİLERİ SAKLAMA SÜRECİNDE YER ALANLARIN İSİMLERİ VE SORUMLULUKLARI

SORUMLU	BİRİM	GÖREV TANIMI
Suna Doğan	İnsan Kaynakları	İK Direktörü
Eda Demirci	İnsan Kaynakları	İK Uzmanı

TABLO 2 – KİŞİSEL VERİLERİ İMHA SÜRECİNDE YER ALANLARIN İSİMLERİ VE SORUMLULUKLARI

SORUMLU	BİRİM	GÖREV TANIMI
Mesut Bayrak	Bilişim Teknolojileri	Bilişim Teknolojileri Lideri

ELEKTRONİK NÜSHADIR. BASILI HALİ KONTROLSÜZ KOPYADIR.