



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Güçlü Güzellik Kozmetik Hizmetleri Ticaret Limited Şirketi

1. BÖLÜM: İMHA POLİTİKASI'NIN NİTELİĞİ VE AMACI

1.1. GİRİŞ

İşbu imha politikası, Güçlü Güzellik Kozmetik Hizmetleri Ticaret Limited Şirketi (kısaca Şirket) olarak veri sorumlusu sıfatıyla elimizde bulduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin Şirket tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve herhangi bir nedenle Şirket nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri tüm [KVKK Metinlerimiz/Politikalarımız](#) ve işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

1.2. TANIMLAR ve İFADELER

Aşağıda tabloda yer alan tanımlar ve ne anlama geldikleri ayrıntılı olarak açıklanmıştır:

Doğrudan tanımlayıcılar	Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılar
Dolaylı tanımlayıcılar	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılar
İlgili kişi	Kişisel verisi işlenen gerçek kişi
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kanun	07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu

Yönetmelik	28.10.2017 tarihli ve 30224 sayılı Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği
Kurul	Kişisel Verileri Koruma Kurulu
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
Gizlilik Ve Kişisel Verilerin Korunması Politikası	www.aquaguzellik.com adresinden ve Şirket'ten ulaşılabilecek, Şirket elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politika
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi

2. BÖLÜM: ORTAMLAR VE GÜVENLİK TEDBİRLERİ

2.1. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Şirket her halde veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri Kanun'a, [Gizlilik ve Kişisel Verilerin Korunması Politikası](#) ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak işlemek ve korumaktadır.

Matbu ortamlar	Verilerin kâğıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
Yerel dijital ortamlar	ŞİRKET bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler, yetkili bilgisayarlar, kamera sistemleri gibi sair dijital ortamlardır.
Bulut ortamlar	ŞİRKET bünyesinde yer almamakla birlikte, ŞİRKET'nin kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

2.2. ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

Şirket, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düşüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

2.2.1. Teknik Tedbirler

Şirket, 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.
- Şirket bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.

2.2.2. İdari Tedbirler

Şirket, 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 yapılmakta, iş sözleşmelerine/yönetmeliklere bu yönde cezai hüküm konulmaktadır.
- 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.

2.2.3. Şirket İçi Denetim

Şirket, Kanun'un 12. maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Gizlilik Ve Kişisel Verilerin Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilmektedir.

Denetim sırasında ya da sair bir şekilde Şirket sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, Şirket bu durumu en kısa sürede ilgisine ve Kurula bildirimde bulunur.

3. BÖLÜM: KİŞİSEL VERİLERİN İMHASI

3.1. SAKLAMA VE İMHA NEDENLERİ

3.1.1. Saklama Nedenleri

Şirket bünyesinde tutulan ve ayrıca Web Site'sinde mevcut [Aydınlatma Metni](#), Gizlilik Ve Kişisel Verilerin Korunması Politikası (www.aquaguzellik.com adresinden ulaşabilirsiniz) uyarınca, hem bu metinler içerisinde hem de aşağıda belirtilen amaç ve nedenlerle saklanmaktadır.

Ek olarak saklamayı gerektiren hukuki amaç ve sebepler aşağıdaki gibidir:

- Ticari faaliyetlerin sürdürülebilmesi,
- Hukuki yükümlülüklerin yerine getirilebilmesi,
- Çalışan haklarının ve yan haklarının planlanması ve ifası,
- Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi,
- Müşteri ilişkilerini yönetebilmesi,
- Bir hakkın tesisi, kullanılması veya korunması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaati için veri işleminin zorunlu olması,
- Mevzuatta kişisel verilerin saklanması için açıkça öngörülmesi,
- KVKK Madde 5/2'de sayılan şartlardan birinin varlığından söz edilemeyecek durumlarda, saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması,
- Fiziksel mekan güvenliğinin temini,
- Ücret politikasının yürütülmesi,

sebepleriyle, ilgili Kanun ve Yönetmeliğin çizdiği sınırlar çerçevesinde kişisel veriler saklanmaktadır.

Hukuki Dayanaklar (Sınırlı olmamak üzere):

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,

-6098 sayılı Türk Borçlar Kanunu,5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

-5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

-6331 sayılı İş Sağlığı ve Güvenliği Kanunu,

-4857 sayılı İş Kanunu, 3308 sayılı Mesleki Eğitim Kanunu, 5434 sayılı Emekli Sağlığı Kanunu, 2828 sayılı Sosyal Hizmetler Kanunu,

-İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik ile sair her türlü yasal dayanak.

3.1.2. İmha Nedenleri

Şirket bünyesinde bulunan kişisel veriler;

-İlgili kişinin, Kanun'un 11. maddesindeki haklarını kullanmak suretiyle verilerinin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabulü,

-Veri sorumlusunun, ilgili kişinin Kanun'un 11. maddesindeki haklarını kullanarak başvurmaya karşın cevap vermemesi, başvuruyu reddetmesi ya da cevabın yetersiz olması sebepleriyle ilgili kişinin Kurul'a şikayette bulunması ve Kurul tarafından uygun bulunması,

- Kişisel verinin açık rıza ile işlenmiş bulunup, ilgili kişinin bu açık rızasını geri alması,

-Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

-Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

-Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

-Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması halinde işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.

3.2. İMHA YÖNTEMLERİ

Şirket, yukarıda belirtilen **İmha Nedenleri** doğrultusunda ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde kişisel verileri re'sen siler, yok eder veya anonim hale getirir.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

3.2.1. Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Karartma	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. 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 görünmez hale getirilmesi şeklinde yapılır.
Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Yazılımdan Güvenli Olarak Silme	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

3.2.2 Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel Yok Etme	Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel Yok Etme	Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.
De-Manyetize Etme (Degauss)	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
Üzerine Yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Yazılımdan Güvenli Olarak Silme	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

3.2.3. Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri Çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabilir gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.
Bölgesel Gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumunda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
Genelleştirme	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiksel veri haline getirilmesi işlemidir.
Alt ve Üst Sınır Kodlama / Global Kodlama	Belli bir değişken için o değişkene ait aralıklar tanımlanarak sınıflandırılır. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler sınıflandırılır. Aynı sınıf içinde kalan değerler birleştirilir.
Mikro Birleştirilme	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olduğundan, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
Veri Karıştırma 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.

Şirket, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. Şirket, bu anonimleştirme yöntemlerini kullanırken K-Anonimlik (K-Anonymity), L-Çeşitlilik (L-Diversity) ve T-Yakınlık (T-Closeness) istatistik yöntemlerini kullanabilir.

3.3. SAKLAMA VE İMHA SÜRELERİ

3.3.1. Saklama Süreleri

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	İş ilişkisinin sona ermesinden itibaren 10 Yıl muhafaza edilir. Zorunlu saklama süresi sonunda imha edilir.
Çalışan	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 (on) yıl müddetle muhafaza edilir.
İş Ortağı/Çözüm Ortağı/ Danışman	İş Ortağı/Çözüm Ortağı/ Danışman ile ŞİRKET arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	İş Ortağı/Çözüm Ortağı/ Danışmanın, ŞİRKET 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.
Ziyaretçi	ŞİRKET'e ait fiziki mekana girişte alınan Ziyaretçiye ait ad, soyad, ile kamera kayıtları, telefon aramalarında alınan ses kayıtları	2 yıl süre ile saklanır.
İnternet Sitesi Ziyaretçisi	İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	2 yıl süre ile saklanır.

Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.
Müşteri	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, aldığı hizmetle alakalı gerekli sağlık bilgileri	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.
Müşteri-Ziyaretçi	Kamera görüntüleri	15 gün süre ile saklanır.
ŞİRKET'in İşbirliği İçinde Olduğu Kurum/Firmalar (Tedarikçi, Fason Üretici, Bayi/ Franchise	ŞİRKET'in İşbirliği İçinde Olduğu Kurum/Firmalar ile ŞİRKET arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, ŞİRKET'in İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri	ŞİRKET'in İşbirliği İçinde Olduğu Kurum/Firmaların, ŞİRKET 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.

* 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.

3.3.2. İmha Süreleri

Şirket, Kanun, ilgili mevzuat, Şirket Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanununun 13. maddesine istinaden Şirket'te ve Site'de mevcut [KVKK Başvuru Formunu](#) kullanmak sureti ile başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Şirket'in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak başvuru yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.
2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanununun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

3.4. PERİYODİK İMHA

Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri 01.06.2022 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

3.5. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

Şirket, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Politikalarına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

3.5.1. Teknik Tedbirler

- ŞİRKET, işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
- ŞİRKET, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- ŞİRKET, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
- ŞİRKET, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

3.5.2. İdari Tedbirler

- ŞİRKET, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- ŞİRKET, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- ŞİRKET, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- ŞİRKET, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklerle uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- ŞİRKET, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

4. BÖLÜM: KİŞİSEL VERİ KOMİTESİ

ŞİRKET bünyesinde bir Kişisel Veri Komitesi kurar. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka, Gizlilik Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi bir yönetici, bir idari uzman ve bir teknik uzman olmak üzere üç kişiden oluşur. Kişisel Veri Komitesinde görevli Şirket çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

Unvan	Görev Tanımı
Kişisel Veri Komitesi Yöneticisi	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Gizlilik Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.

KVKK Görevlisi (Teknik ve İdari)	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.
Bilgi Teknolojileri Görevlisi	Kişisel veri saklama ve imha politikası uygulama sorumlusu verilerin saklama süresine uygunluğunu sağlama ve periyodik imha süresi içinde imha sürecini yönetmek
Mali İşler Müdürü, Mali İşler Mali İşler Departmanı	Kişisel veri saklama ve imha politikası uygulama sorumlusu verilerin saklama süresine uygunluğunu sağlama ve periyodik imha süresi içinde imha sürecini yönetmek

5. BÖLÜM: GÜNCELLEME VE UYUM

Şirket, Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.

İşbu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

5.1 DEĞİŞİKLİK NOTLARI

30.12.2021	Kişisel Veri Saklama ve İmha Politikası yayınlanmıştır.
-------------------	---

* eski tarihli bir değişiklik bulunmamaktadır.*