NUTRILINE
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İçindekiler

BİRİNCİ BÖLÜM
§ 1.GİRİŞ

1.1. Politikanın Kapsamı

İşbu Politika, Şirketin tüm kişisel veri işleme faaliyetlerinde uygulanır ve Şirketin faaliyetlerinde görev alan herkes için bağlayıcı ve yol göstericidir.

1.2. Politikanın Amacı

İşbu Politika'nın temel amacı, hukuka ve Kanun'un amacına uygun olarak kişisel verilerin saklanması ve imhasına yönelik sistemler konusunda açıklamalarda bulunmak, bu kapsamda Şirket paydaşları, Şirket yetkilileri, Şirket iş ortakları, çalışan, çalışan adayları, ziyaretçiler, Şirket müşterileri, potansiyel müşteriler ve üçüncü kişiler başta olmak üzere tüm kişi gruplarına ilişkin kişisel veri saklama ve imha faaliyetinin hukuka ve dürüstlük kurallarına uygun olarak yürütülmesi için uyulması gereken genel usul ve esasları belirlemektir.

1.3.Tanımlar

İşbu Politika'da yer verilen kavramlar aşağıda belirtilen anlamları ifade eder:

Alıcı grubu	:	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık rıza	:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim hale getirme	:	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Çalışan	:	Şirket personeli.
Dijital ortam	:	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
İlgili kişi	:	Kişisel verisi işlenen gerçek kişi.
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 kişiler.

İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	:	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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.
Kişisel veri	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel veri envanteri	:	Şirket'in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı envanter.
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul	:	Kişisel Verileri Koruma Kurulu
Periyodik İmha	:	Kanunda yer alan kişisel verilerin işlenme 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.

Politika	:	Kişisel verileri saklama ve imha Politikası.
Veri sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Veri kayıt sistemi	:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

1.5. Politikanın Yürürlüğü

İşbu Politika Şirket tarafından düzenlenerek 20.12.2020 tarihinde yürürlüğe girmiştir. Politikadaki değişikliklere ilişkin kayıtlar beşinci bölümde yer almaktadır.

İKİNCİ BÖLÜM
§ 2. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

2.1. Kişisel Verilerin Saklandığı Ortamlar

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklere 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 eder ve kişisel verileri Kanuna, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Politikaya uygun olarak saklar ve korur.

a) Matbu ortamlar : Verilerin kâğıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.

b) Yerel dijital ortamlar : Şirket bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır.

c) Bulut ortamlar : Şirket bünyesinde yer almamakla birlikte, Şirket'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

2.2. Ortamların Güvenliğinin Sağlanması

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 düştüğü 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:

- Bilişim sistemlerinin ve ağ güvenliğinin sağlanması için mevcut teknolojik gelişmeler göz önüne alınarak ağ güvenliği ve uygulama güvenliği sağlanır. Bu kapsamda güncel antivirus ve/veya güvenlik duvarları kullanılır.
- Sızma (penetrasyon) testleri ile bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınır. Bu testler, Şirket tarafından belirlenecek makul periyotlarla tekrar edilir.
- Şirket tarafından kullanılan bilişim sistemlerinde erişim yetkisi düzenlemesi yapılır. Erişim yetkileri güncel tutulur, görev değişikliği anında ilgili erişim yetkileri güncel duruma uygun hale getirilir.
- Bilişim sistemleri üzerinde yapılan her türlü işleme ilişkin güvenilir, sonradan değiştirilemez log kayıtları tutulur.
- Kullanılan bilişim sistemleri her daim güncel tutulur. Dijital güvenlik ve gizliliğe ilişkin güncel teknolojik gelişmeler takip edilir ve bu kapsamda gerekli önlemler alınır. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınır.
- Bilişim sistemlerindeki verilere ulaşmaya yetkili tüm kullanıcı hesapları şifrelenir. Şirket içerisinde kullanıcıların şifrelerini ve/veya hesaplarını paylaşmaları engellenir. Fiziksel olarak saklanan kişisel verilerin saklama ortamları kilitli tutulur. Gerektiğinde veri maskeleme sistemi kullanılır.

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 yapılır.

- Gerektiğinde, bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması kapsamında hukuki ve teknik danışmanlık hizmeti alınır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde kişisel verilerin korunması amacıyla ilgili sözleşmelere veri güvenliğine ilişkin hükümler eklenir ve/veya ayrıca gizlilik sözleşmeleri veya taahhütnameleri imzalanır.
- Şirket içinde kişisel verilere ulaşmaya yetkili kişilerin bilgi güvenliğine ve gizliliğine ilişkin taahhütnameleri imzalaması sağlanır.
- Kişisel veri güvenliğine ilişkin politikalar belirlenir. Politikaların güncel tutulması ve uygulanması için gerekli aksiyonlar alınır.
- Kişisel verilere ilişkin sorunların hızlı bir şekilde Şirket içindeki ilgili birimlere raporlanması sağlanır.
- Kişisel verilerin tutulduğu ortamların gerek yetkisiz erişimlere gerekse dış etkenlere karşı güvenliği sağlanır.

2.2.3. Şirket İçi Denetim

Şirket, Kanun'un 12. maddesi uyarınca Kanun hükümlerinin ve işbu Politika ile Kişisel Verilerin İşlenmesi ve 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 giderilir.

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 ilgilisine ve kurula bildirir.

ÜÇÜNCÜ BÖLÜM
§ 3. KİŞİSEL VERİLERİN İMHASI

3.1. Saklama ve İmha Sebepleri

3.1.1. Saklama Sebepleri

Şirket kişisel verileri ancak aşağıda sayılan işleme sebeplerinden en az birinin bulunması halinde saklar.

a) İlgili kişinin açık rızasının bulunması,
b) Kanunlarda açıkça öngörülmesi,
c) 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,
d) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

e) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
f) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
g) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
h) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel veriler ancak işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir.

Bu süreler ilgili kişisel verinin niteliği, işleme amacı ve hukuki sebebi dikkate alınarak Şirket'in kişisel veri envanterinde belirlenir.

3.1.2. İmha Nedenleri

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Şirket tarafından re'sen ya da ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir.

3.2. İmha Yöntemleri

İmha gerekliliği ortaya çıktığı taktirde Şirket verinin niteliği, saklandığı ortam, gizlilik derecesi ve risk seviyesi hususlarını göz önüne alarak silme, yok etme ve imha etme yöntemlerinden birini seçer ve uygular.

Şirket tarafından kullanılan başlıca silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır.

3.2.1.1 Silme Yöntemleri

Silme işlemi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Matbu ortamda tutulan kişisel veriler için 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 ilgili kullanıcılar tarafından geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilmesi şeklinde yapılır.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri		
Yazılımdan güvenli olarak silme	:	Yerel dijital ortamlarda tutulan kişisel veriler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

3.2.1.2. Yok Etme Yöntemleri

Yok etme işlemi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Matbu ortamda tutulan kişisel veriler için 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 için 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.

3.2.1.3. 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 bir kaçının çıkarılmasıdır.

Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği 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 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 / Global kodlama	:	Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir. Aynı kategori 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 olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
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.

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.

Şirket, ilgili kişinin talebini, Şirketin menfaatini ve imhaya konu verinin niteliğini değerlendirerek en uygun, elverişli ve orantılı imha yöntemini seçer.

3.3. Saklama ve İmha Süreleri

3.3.1. Saklama Süreleri

Kişisel veriler ancak işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir.

Bu süreler, ilgili kişisel verinin niteliği, işleme amacı ve hukuki sebebi dikkate alınarak Şirket'in kişisel veri envanterinde belirlenir.

Saklama süreleri belirlenirken uygulanabilir hukukta yer alan şikayet, zamanaşımı, hak düşürücü ve benzeri süreler ile saklama yükümlülüğünün düzenlendiği hallerde belirlenen bu süreler dikkate alınır.

3.3.2. İmha Süreleri

Şirket, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması 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, Kanun'un 13. maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) 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'ın talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.
b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa; bu talep Şirket tarafından Kanun'un 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde ilgilinin talep ettiği iletişim aracıyla bildirilir.

İlgili kişiye verilecek cevaplar Kişisel Verilerin İşlenmesi ve Korunması Politikasında yer alan düzenlemelere ve Kurul kararlarına uygun olmalıdır.

3.4. Periyodik İmha

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda imha yükümlülüğü doğar. Şirket, imha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

Her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

3.5. İmha İşleminin Hukuka Uygunluğunun Denetimi

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

Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla en az aşağıdaki idari ve teknik tedbirler alır.

3.5.1. Teknik Tedbirler

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

3.5.2. İdari Tedbirler

- Şirket, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- Şirket, 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.
- Şirket, 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.
- Şirket, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- Şirket, 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.

DÖRDÜNCÜ BÖLÜM
§ 4. KİŞİSEL VERİ KOMİTESİ

Şirket bünyesinde bir Kişisel Veri Komitesi kurar. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka ve Şirket Politikalarına uygun olarak işlenmesi, saklanması ve imhası için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi en az biri İnsan Kaynakları Sorumlusu olmak üzere, Şirket tarafından seçilen üç kişiden oluşur. Komiteye seçilen kişiler bir yönetici ve iki uzman olarak çalışır. Görevlendirmeler Şirket tarafından yapılır. Kişisel Veri Komitesinde görevli yönetici ve uzmanların görev tanımları aşağıda belirtilmiştir:

Unvan		Görev Tanımı
Kişisel Veri Komitesi Yöneticisi	:	Politika ve prosedürleri hazırlamak ve yürütmek; Kanun'a uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
KVK Uzmanı (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; Kişisel Veri Komitesi Yöneticisi tarafından verilen sair görevlerin yerine getirilmesinden sorumludur.

BEŞİNCİ BÖLÜM
§ 5. GÜNCELLEME VE UYUM

İşbu Politika, Kanunda ya da sair mevzuatta yapılan değişiklikler nedeniyle, Kurul kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda güncellenir. İşbu Politikada yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar Politikanın sonunda açıklanır.

5.1. Değişiklik Notları

20.12.2020 : Kişisel Verilerin İşlenmesi ve Korunması Politikası yayınlanmıştır.

daha eski tarihli bir değişiklik bulunmamaktadır.