Kişisel Veri Saklama ve İmha Politikaları

1. GİRİŞ

Kişisel Veri Saklama ve İmha Politikaları ('**Politika**'), MNG Faktoring Anonim Şirketi ('**Şirket**') tarafından 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ('**Kanun**') 7 nci maddesi ile 28.10.2017 tarihli ve 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ('**Yönetmelik**') uyarınca hazırlanmıştır.

Bu Politika, Şirket tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket' in veri sorumlusu sıfatıyla hareket ettiği her türlü faaliyeti kapsamında işlenen kişisel veriler bu Politika kapsamında olup Şirket' e ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanacaktır.

2. TANIMLAR

Politikada kullanılan ifadelerin ve terimlerin anlamları ve bunlara ilişkin açıklamalar aşağıda yer almaktadır.

Kurum : Kişisel Verileri Koruma Kurumu.
Kurul : Kişisel Verileri Koruma Kurulu.
Veri Sorumlusu : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Veri İşleyen : Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
Açık rıza / : Belirli bir konuya ilişkin bilgilendirmeye dayanan ve özgür iradeyle açıklana rıza.
Alıcı grubu : Kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Anonim hale getirme : Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkinlendirilmeyecek hale getirilmesi.
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 Şirket organizasyonu içerisinde verilen yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.
İmha : Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işleml eri.
Kayıt ortamı : Tamamen veya kısmen otomatik ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenenm kişisel verilerin bulunduğu her türlü ortam.
Kişisel veri : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Veri İşleme Envanteri : İş süreçlerine bağlı olarak gerçekleştirilen kişisel veri işleme faaliyetlerini; işleme amaçları, veri kategorisi, aktarılan alıcı gurbu ve veri konusu kişi grubuyla ilişkilendirilerek oluşturulan ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandıran envanter.
Kayıt Veri Saklama ve İmha Politikası : Kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak olan politika.
Kayıt verilerin 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 üzerinden gerçekleştirilen her türlü işlem.

Maskeleme : Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri.
Periyodik imha : Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda işlemleri Kişisel Veri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Veri kayıt sistemi : Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

3. ROLLER ve SORUMLULUKLAR

Şirketin tüm birimleri ve çalışanları kişisel verilerin mevzuata ve şirket politikalarına uygun şekilde işlenmesi ve saklanması, hukuka aykırı işleme ve erişim faaliyetlerinin engellenmesi, kişisel verilere ilişkin teknik ve idari tedbirlerin uygulanması, şirket çalışanlarının eğitim ve farkındalığının arttırılması ve bu hususlarda ilgili birimlere destek verilmesi konularında sorumludur.

Kişisel verileri saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımları aşağıdaki gibidir:

Unvan	Birim	Görev
Uyum	İç Kontrol ve Risk Yönetimi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Hukuk	Hukuk Birimi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi ile ilgili Uyum ekibi ile birlikte sorumludur.
Bilgi Teknolojileri Müdürü ve Bilgi Teknolojileri Müdürü tarafından yetkilendirilen ilgili kişiler	Bilgi Teknolojileri Departmanı (IT)	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Departman/Birim Yöneticileri	Tüm departmanlar/birimler	Çalışanların Politikaya uygun hareket etmesinden ve Politikanın yürütülmesinden sorumludur.
Çalışanlar	Tüm departmanlar/birimler	Kendilerine verilen görev ve yetkiler kapsamında gerçekleşen kişisel veri işleme faaliyetleri bakımından ve bu tabloda belirtilen diğer yetkililer tarafından Politika kapsamında kendilerine verilen talimatlar doğrultusunda Politikayı uygulamak konusunda sorumludur.

4. KAYIT ORTAMLARI

Şirket, Kanun'a uygun olarak gerçekleştirmekte olduğu veri işleme faaliyetleri kapsamında elde ettiği kişisel verileri, işleme amacının gerektirdiği ölçü ile sınırlı olmak kaydıyla muhafaza etmektedir. Bu kapsamda elde edilen kişisel veriler, MNG Faktoring tarafından fiziki ve elektronik ortamda saklanmaktadır.

5. KİŞİSEL VERİLERİN SAKLANMASINI ve İMHASINI GEREKTİREN SEBEPLER

Kişisel veriler ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süreler boyunca Şirket politikalarına uygun olarak saklanır ve işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde resen veya ilgili kişinin talebi üzerine imha edilir.

A. Saklama Sebepleri

Şirket faaliyetleri kapsamında işlenen kişisel veriler aşağıdaki sebeplerle saklanır:

- Kanunlarda açıkca öngörülmesi,
- Şirketin hukuki yükümlülüklerini yerine getirilmesi için veri işlemenin zorunlu olması,
- İnsan kaynakları süreçlerinin yürütülmesi,
- Şirket içi ve bağımsız disiplin ve denetim faaliyetlerinin gerçekleştirilmesi,
- Şirketin taraf olduğu/olacağı sözleşmelerin kurulması ve ifası,
- Şirketin faaliyetlerine ilişkin raporların hazırlanması,
- Müşteri ve tedarikçi ilişkilerinin yönetilmesi,
- Şirket faaliyetleri çerçevesinde kurumsal iletişimin sağlanması,
- Şirketin hukuki menfaatinin korunması ve hukuki ispat yükümlülükleri,
- Kişisel verinin ilgili 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.

B. İmha sebepleri

Şirket faaliyetleri kapsamında saklanan kişisel veriler aşağıdaki sebeplerle MNG Faktoring tarafından kendiliğinden veya ilgili kişinin talebi üzerine imha edilir:

- İlgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın veya sebebin ortadan kalkması,
- Kişisel veri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- İlgili kişinin imha talebinin Şirket tarafından kabul edilmesi,
- İlgili kişinin reddedilen imha talebinin Kurul tarafından uygun bulunması,
- Saklamayı gerektiren azami sürenin geçmiş olması ve daha uzun süre saklamayı haklı kılacak herhangi bir geçerli sebebin bulunmaması.

6. TEKNİK ve İDARİ TEDBİRLER

Şirket tarafından kişisel verilerin korunması yükümlülükleri kapsamında uygulanan teknik ve idari tedbirler aşağıdadır.

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır,
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır,
- Anahtar yönetimi uygulanmaktadır,
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur,
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır,

- Çalışanlar için yetki matrisi oluşturulmuştur,
- Erişim logları düzenli olarak tutulmaktadır,
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır,
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır,
- Gizlilik taahhütnameleri yapılmaktadır,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır,
- Güvenlik duvarları kullanılmaktadır,
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir,
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir,
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir,
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır,
- Kişisel veri güvenliğinin takibi yapılmaktadır,
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır,
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır,
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır,
- Kişisel veriler mümkün olduğunca azaltılmaktadır,
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır,
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır,
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır,
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır,
- Mevcut risk ve tehditler belirlenmiştir,
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır,
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir,
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir,
- Saldırı tespit ve önleme sistemleri kullanılmaktadır,
- Sızma testi uygulanmaktadır,
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir,
- Şifreleme yapılmaktadır,
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır,
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır,
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır,
- Veri kaybı önleme yazılımları kullanılmaktadır.

7. İMHA TEKNİKLERİ

Şirket tarafından kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi sürecinde aşağıdaki imha yöntemleri ve tedbirleri uygulanacaktır.

A. Silme

Silme işlemi uygulanacak kişisel veriler belirlendikten sonra bu kişisel verilere erişimi olan ilgili kullanıcılar ve bu kullanıcıların erişim yetkileri ve yöntemleri belirlenir. İlgili kullanıcıların kişisel

verilere ilişkin erişim, geri getirme ve tekrar kullanma yetki ve yöntemlerinin ortadan kaldırılması yoluyla silme işlemi gerçekleştirilir.

Kişisel verilerin bulunduğu ortamlara göre uygulanabilecek silme yöntemleri aşağıdadır.

Veri Kayıt Ortamı	Silme Yöntemi
Elektronik Ortamlar	Veritabanı veya sistem yöneticisi ya da kullanıcının kendisi tarafından silme komutlarının veya yazılımlarının kullanılması ya da ilgili kullanıcıların erişim ve/veya kullanım yetkilerinin kaldırılması
Elektronik Olmayan Ortamlar	Silme, çizme ve/veya boyama yöntemleriyle karartma

B. Yok Etme

Yok etme işlemi uygulanacak kişisel veriler ve bunların kayıt ortamları belirlenir. Kişisel veriler ve gerekli hallerde bu kişisel verilerin bulunduğu kayıt ortamları hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmek suretiyle yok etme işlemi gerçekleştirilir.
Kişisel verilerin bulunduğu ortamlara göre uygulanabilecek yok etme yöntemleri aşağıdadır.

Veri Kayıt Ortamı	Yok Etme Yöntemi
Elektronik Ortamlar	Fiziksel yok etme (eritme, öğütme, yakma), de-manyetize etme veya üzerine yazma
Elektronik Olmayan Ortamlar	Kırpma veya öğütme, yakma, toz haline getirme

C. Anonim Hale Getirme

Kişisel veriler aşağıdaki yöntemlerden bir veya birkaçı kullanılmak suretiyle başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmek suretiyle anonim hale getirilir.

- Değişkenleri çıkartma
- Kayıtları çıkartma
- Alt ve üst sınır kodlama
- Bölgesel gizleme
- Örnekleme
- Mikro-Birleştirme
- Veri Değiş-Tokuşu
- Gürültü Ekleme
- Tekrar Örnekleme
- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

8. SAKLAMA ve İMHA SÜRELERİ

Saklama süreleri sona eren kişisel veriler için Şirket tarafından en geç saklama süresinin bitimini takip eden ilk periyodik imha süresinde silme, yok etme veya anonim hale getirme işlemleri gerçekleştirilir.

	Kayıt Türü	Saklama Süresi
Muhasebe ve Finans	Ticari borç hesapları	Finansal yılın sona ermesinden itibaren 10 yıl
	Alacak hesapları	Finansal yılın sona ermesinden itibaren 10 yıl
	Tedarikçi faturaları ve ilgili belgeler	Finansal yılın sona ermesinden itibaren 10 yıl
	Defteri kebir	Finansal yılın sona ermesinden itibaren 10 yıl
	Finansal beyannameler	Finansal yılın sona ermesinden itibaren 10 yıl
	Yıllık denetim raporları ve finansal beyannameler	Finansal yılın sona ermesinden itibaren 10 yıl
	Yıllık plan ve bütçeler	Finansal yılın sona ermesinden itibaren 10 yıl
	Banka hesap özetleri	Finansal yılın sona ermesinden itibaren 10 yıl
	Çalışan harcama raporları	Finansal yılın sona ermesinden itibaren 10 yıl
Sözleşmeler	Sözleşmeler	Sözleşme süresi boyunca + 10 yıl
Kurumsal Kayıtlar	Kurumsal kayıtlar (toplantı defterleri, imzalı Yönetim Kurulu toplantı tutanakları, ana sözleşme, iç tüzükler, yıllık kurumsal kayıtlar)	Süresiz (Şirket'in faaliyette kaldığı süre boyunca + 10 yıl)
	Yönetim kurulu defterleri	10 yıl
	Lisans ve izinler	İlgili lisans veya iznin sona ermesinden itibaren 10 yıl
	Fikri mülkiyet haklarına ilişkin kayıtlar ve ilgili dokümanlar	Süresiz Şirket'in faaliyette kaldığı süre boyunca + 10 yıl)
Hukuki Kayıtlar	Hukuki bilgi notları ve görüşler	İlgili konunun sona ermesinden veya yeni görüş/not alınmasından itibaren 10 yıl
	Dava dosyaları	Temyiz süresinin sona ermesi itibarıyla 10 yıl
	Yargısal talepler, ibra, feragat ve uzlaşmalar	Kesinleştiği tarih itibariyle 10 yıl
Sigorta Kayıtları	Sigorta poliçeleri ve ilgili dava dosyaları, diğer sigorta kayıtları ve ilgili dava dosyaları, sigortalara ilişkin ibra ve uzlaşmalar	İbra veya uzlaşmanın kesinleştiği veya poliçenin sona erdiği tarihten itibaren 10 yıl
Tedarikçi Verileri	Ticari sözleşmelerin akdi kapsamında tedarikçilerden alınan veriler	Sözleşmesi süresi boyunca + 10 yıl
Müşteri Verileri	Müşteri ilişkisinin kurulması ve devamı boyunca alınan veriler	Müşteri ilişkisi boyunca + 10 yıl
Yasal Yükümlülükler	Yasal yükümlülükler doğrultusunda resmi bildirimleri amacıyla toplanan veriler	Bildirimin gerçekleştirilmesinden itibaren 10 yıl

	Kayıt Türü	Saklama Süresi
Çalışan ve Çalışan Adayları Kayıtları	Aşağıdakiler de dâhil olmak üzere çalışan özlük dosyaları: - iş başvuruları/özgeçmiş - referans kontrolleri - iş tanımları - tazminat geçmişi - performans değerlendirmeleri - disipline ilişkin bilgiler - terfiler - feshe ilişkin belgeler	İş sözleşmesi süresi boyunca + 10 yıl
	Aşağıdakiler de dâhil olmak üzere iş başvurusu reddedilen çalışan aday bilgileri: - mülakat notları - özgeçmişler - iş teklifleri - başlangıç değerlendirmeleri - işe alım sürecinde yapılan ön eleme	İlgili işlemin sona ermesinden itibaren 1 yıl
	Çalışan sağlık kayıtları (ayrı ve gizli dosya)	İş sözleşmesi süresi boyunca + 15 yıl
	Adli sicil kayıtları (ayrı ve gizli dosya)	İş sözleşmesi süresi boyunca
	Çalışan eğitimleri	İş sözleşmesi süresi boyunca + 10 yıl
	İş sözleşmeleri	İş sözleşmesi süresi boyunca + 10 yıl
	Emeklilik ve emekli aylığı düzenlemeleri	İlgili düzenlemenin veya hak edişin sona erdiği tarihten itibaren 10 yıl

9. PERİYODİK İMHA

Kişisel verilere ilişkin periyodik imha süresi 6 aydır. Her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

10. İMHA KAYITLARI

Politika kapsamında kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler saklı kalmak üzere en az üç yıl süreyle saklanır. Bu kayıtların tutulması ve saklanması sürecinin yönetimi ve yürütülmesinden Şirket Bilgi Güvenliği sorumludur.

11. YÜRÜTME ve YÜRÜRLÜK

Bu politikanın ve bağlantılı referans dokümanların uygulatılmasından Yönetim Kurulu sorumlu olup, ilgili süreçlerin sağlıksız ve eksiksiz yürütülmesinden Genel Müdür ve İç Kontrol ve Risk Yönetimi Bölümü ve Hukuk Birimi müteselsilen sorumludur. Bu politika kapak sayfasında belirtilen tarih itibariyle yürürlüğe girer.

12. DAĞITIM ve GÜNCELLEME

Doküman ilgili kullanıcıların erişimine açık olarak Şirket' in web sitesi üzerinde bulundurulur. Yılda bir ve/veya gerektiğinde Hukuk Birimi ve İç Kontrol ve risk Yönetimi Bölümü tarafından, diğer birimlerden gelen görüş ve istekler de göz önünde bulundurularak gözden geçirilecek ve gerekirse güncellemesi yapılacaktır. Doküman üzerinde değişiklik yapıldıysa, son hali Yönetim Kurulu' na onay için sunulacak, onay alımından sonra yayımlanarak yürürlüğe girecektir.