MAYGOLD PETROL
ANONİM ŞİRKETİ
SAKLAMA VE İMHA POLİTİKASI

İÇİNDEKİLER

MAYGOLD PETROL ANONİM ŞİRKETİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

Kişisel verilerin korunması, Maygold Petrol Anonim Şirketi ("**Şirket**") için büyük önem arz etmekte olup, bu konuda azami hassasiyet gösterilmektedir. Bu doğrultuda, kişisel verilerin kişilerin beklentileri ile tutarlı bir şekilde ve yasalara uygun olarak işlenmesi, Şirketimizin temel yapı taşlarından biridir.

Bu bakımdan Şirketimiz, faaliyetleri sırasında elde etmiş olduğu kişisel verileri başta Anayasa olmak üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**"), Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") ve diğer ilgili mevzuata uygun şekilde hazırlanan işbu Kişisel Veri Saklama ve İmha Politikası'nda ("**Politika**") belirtilen genel prensipler ve düzenlemelere uygun şekilde saklamakta ve imha etmektedir.

2. POLİTİKA'NIN AMACI VE KAPSAMI

İşbu Politika ile Şirketimiz, Kanun kapsamındaki kişisel veri işleme faaliyetlerine konu gerçek kişi verilerinin saklanması ve imha edilmesine ilişkin Şirket'in genel ilke ve prensiplerinin ortaya konulması ve bu hususlarla ilgili mevzuatla belirlenen yükümlülüklerin yerine getirilmesi hedeflemiştir.

İşbu Politika, Şirketimizin Kanun kapsamındaki veri işleme faaliyetlerine konu tüm kişisel verileri kapsamaktadır. Ayrıca, işbu Politika'da aksi belirtilmedikçe, Politika ile atıf yapılan dokümanlar hem basılı hem de elektronik kopyaları kapsamaktadır.

3. TANIMLAR

İşbu Politika'da içerik aksini gerektirmedikçe:

"**Açık Rıza**"	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza,
"**Alıcı Grubu**"	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi,
"**Anayasa**"	Türkiye Cumhuriyeti Anayasası,
"**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,
"**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 (örn. ad-soyad, TCKN, e-posta, adresi, doğum tarihi, kredi kartı numarası, banka hesap numarası - *Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir*),
"**Kişisel Veri Sahibi**"	Kişisel verisi işlenen gerçek kişi,
"**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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,
"**Kurul**"	Kişisel Verileri Koruma Kurulu,
"**Özel Nitelikli 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,
"**Periyodik İmha**"	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda işbu Politika'da belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi,
"**Veri Sorumlusu**"	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten kişi

anlamına gelmektedir.

4. POLİTİKA İLE DÜZENLENEN KAYIT ORTAMLARI

Şirketimiz, Kanun kapsamındaki veri işleme faaliyetlerine konu tüm kişisel verileri, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu ve aşağıda belirtilen ortamlarda saklamaktadır:

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşımı vb.)	Kağıt
Yazılımlar (ofis yazılımları, portal, İYS, VERBİS)	Manuel Veri Kayıt Sistemleri (Anket formları, Ziyaretçi Giriş Defteri)
Bilgi Güvenliği Cihazları (Güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyaları, sızıntı testleri, antivirüs vb.)	Yazılı, basılı, görsel ortamlar
Mobil cihazlar (telefon vb.)	
Kişisel bilgisayarlar (Masaüstü, dizüstü)	
Optik diskler (CD, DVD vb.)	
Çıkartılabilir bellekler (USB, Hafıza Kart vb.)	
Yazıcı, tarayıcı, fotokopi makinesi	

5. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

Şirketimiz, kişisel veri işleme faaliyetlerinde aşağıdaki ilkeleri esas almaktadır:

- hukuka ve dürüstlük kuralına uygun olunması,
- kişisel verilerin doğru ve gerektiğinde güncel olmasını sağlama,
- belirli, açık ve meşru amaçlarla işleme,
- işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ve
- ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme.

Şirketimiz, kişisel verileri, yukarıda bahsi geçen ilkelerle uyumlu şekilde, Maygold Petrol Kişisel Verilerin Korunması ve İşlenmesi Politikası ile Maygold Petrol Çalışan Kişisel Verilerinin Korunması ve İşlenmesi Politikası'nın ilgili maddelerinde yer alan kişisel veri işleme amaçlarıyla ve aşağıda belirtilen Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarına istinaden kişisel verileri saklamakta ve kullanmakta olup, söz konusu şartların tamamının ortadan kalkması halinde, kişisel verileri re'sen veya kişisel veri sahibinin talebi üzerine imha etmektedir.

(a) Kişisel Veri Sahibinin Açık Rızasının Bulunması

Kişisel verilerin işlenme şartlarından biri sahibinin açık rızasıdır. Kişisel veri sahibinin açık rızası belirli bir konuya ilişkin, bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklanmalıdır.

(b) Kanunlarda Açıkça Öngörülmesi

Veri sahibinin kişisel verileri, kanunlarda açıkça öngörülmesi halinde açık rızası alınmadan hukuka uygun olarak işlenebilecektir.

(c) Fiili İmkansızlık Sebebiyle Kişisel Veri Sahibinin Açık Rızasının Alınamaması

Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınamayacak olan kişinin kendisinin ya da başka bir kişinin hayatı veya beden bütünlüğünü korumak için kişisel verisinin işlenmesinin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

(d) Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde kişisel verilerin işlenmesi mümkündür.

(e) Hukuki Yükümlülük

Şirketimizin hukuki yükümlülüklerini yerine getirmesi için veri işlemenin zorunlu olması halinde kişisel veri sahibinin verileri işlenebilecektir.

(f) Kişisel Veri Sahibinin Kişisel Verisini Alenileştirmesi

Veri sahibinin, kişisel verisini kendisi tarafından alenileştirmiş olması halinde ilgili kişisel veriler alenileştirme amacıyla sınırlı olarak işlenebilecektir.

(g) Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir

(h) Şirketimizin Meşru Menfaati İçin Veri İşlemenin Zorunlu Olması

Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketimizin meşru menfaatleri için veri işlemesinin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

Bu doğrultuda, kişisel veri işleme faaliyetinin dayanağı yukarıda belirtilen şartlardan yalnızca biri olabildiği gibi bu şartlardan birden fazlası da aynı kişisel veri işleme faaliyetinin dayanağı olabilmektedir.

6. KİŞİSEL VERİLERİN İMHA EDİLMESİ İŞLEMİ İLE İLGİLİ UYGULANAN YÖNTEMLER VE KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Şirketimiz, Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verileri aşağıdaki yöntemlerle silmekte, yok etmekte veya anonim hale getirilmesi getirmektedir. Şirketimiz, kişisel verilerin imhasında azami dikkat ve özeni göstermektedir. Bu kapsamda Şirketimiz, Kanun'un 12'nci maddesi ve Yönetmelik hükümleri, yukarıda belirtilen genel ilkeler ile işbu Politika ve Kurul kararları uyarınca aşağıda belirtilen hususlar ile ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır. İmha kapsamında gerçekleştirilen tüm işlemler Şirketimiz tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanmaktadır. Şirketimiz, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını teknolojik imkanlar ve uygulama maliyetine göre seçmekte olup, kişisel veri sahibinin talebi halinde uygun yöntemin gerekçesini açıklamaktadır.

(a) Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda Şirketimiz, kişisel verileri silme işlemi için izlenen süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi ve
- İlgili kullanıcıların kişisel veriler kapsamında erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması

Bu kapsamda Şirketimiz, kişisel verileri silme işlemi için aşağıdaki yöntemleri uygulamaktadır:

- Hizmet Olarak Uygulama Türü Bulut Çözümleri

Bulut sisteminde bulunan kişisel veriler, silme komutu verilerek silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmektedir.

- Fiziki Ortamda Bulunan Kişisel Veriler

Fiziki ortamda bulunan kişisel veriler, karartma yöntemi kullanılarak silinmektedir. Karatma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

- **Merkezi Sunucuda Yer Alan Ofis Dosyaları**

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılmaktadır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir.

- **Taşınabilir Medyada Bulunan Kişisel Veriler**

Flash tabanlı saklama ortamlarındaki kişisel veriler şifreli olarak saklanmakta ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.

- **Veri Tabanları**

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmektedir. Anılan işlem gerçekleştirilirken, ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmektedir.

İşleme amacı tamamen ortadan kalkan fiziki ve elektronik ortamdaki kişisel veriler, Kurum tarafından yayımlanan Rehber'e uygun olarak yok edilir veya yine bu Rehber'de öngörülen yöntemlerle anonim hale getirilir. Teknik Birim tarafından gerçekleştirilen tüm silme, yok etme veya anonim hale getirme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Fiziki ortamdaki kişisel veriler bakımından ise bu işlemlerin gerçekleştirildiğine ilişkin tutanak düzenlenir ve Teknik Birim tarafından muhafaza edilir. Elektronik ve fiziki ortamdaki kişisel verilere ilişkin silme, yok etme veya anonim hale getirmeye ilişkin kayıtlar üç yıl süre ile saklanır. Maygold Petrol, kişisel verileri saklama süreleri boyunca sadece ilgili departmanların bu verilere erişimini sağlayacak şekilde "silme"

yöntemini kullanır. Saklama sürelerinin bitmesi ve kişisel verinin saklanmasını gerektirecek herhangi bir başka amacın mevcut olmaması halinde ise anonim hale getirme yöntemini kullanır.

(b) Kişisel Verilerin Yok Edilme Yöntemleri

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimiz, kişisel verilerin yok edilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda Şirketimiz, kişisel verileri yok etme işlemi için aşağıdaki yöntemleri uygulamaktadır:

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilir.

- **Yerel Sistemler**

Söz konusu sistemler üzerindeki kişisel verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

Fiziksel Yok Etme: Optik medya 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. Katı halde olan diskler bakımından üzerine yazma ya da de-manyetize etme işlemi başarılı olmazsa, bu medya da fiziksel olarak yok edilir.

Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

- **Çevresel Sistemler**

Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünlerin, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, SSD, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldü doğrulanarak özelliğine göre yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

Veri kayıt ortamı sabit olan yazıcı, gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Kağıt Ortamlar**

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılığı olduğundan ana ortam yok edilir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- **Bulut Ortamı**

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde, kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemi ise aşağıdaki şekilde gerçekleştirilir:

İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilerek

Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilerek

Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınarak

(c) Kişisel Verilerin Anonim Hale Getirilme Yöntemleri

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, Şirketimiz, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekmektedir. Şirketimiz, kişisel verilerin anonim hale getirilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

7. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Şirketimiz, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi konusunda azami dikkat ve özeni göstermekte olup, Kanun'un 12'nci maddesi ve Yönetmelik hükümleri, yukarıda belirtilen genel ilkeler ile işbu Politika ve Kurul kararları uyarınca aşağıda belirtilen hususlar ile ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır:

TEKNİK TEDBİRLER	İDARİ TEDBİRLER
Bilgi Teknolojileri Sistemleri Maygold Petrol, kişisel veri güvenliğinin sağlanması adına bilgi teknolojileri sistemleri tedarik eden uzman hizmet sağlayıcılarla çalışmaktadır. Bu kapsamda, Şirket'in gereksinimleri ve zafiyetleri güncel olarak takip edilip, gerekli görülen noktalarda destek sağlanmaktadır.	**Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi** Maygold Petrol, kişisel verilerin korunmasına ilişkin olarak, hem genel işleme faaliyetlerine hem de özellik gösteren işleme süreçlerine yönelik politika ve prosedürler belirlenmiştir. Bu kapsamda Şirket başlıca aşağıdaki politikaları yürürlüğe koymuştur: - Kişisel Verilerin Korunması ve Gizliliği Politikası - Kişisel Verilerin Saklanması ve İmhası Politikası - Çerez Politikası Bunlara ek olarak Şirket'in, çalışanlarının ve yöneticilerinin kişisel veri işleme faaliyetlerine ilişkin olarak da daha detaylı iç yönergeleri mevcuttur. Şirket politikalarını, prosedürlerini ve iç yönergelerini meydana gelen mevzuat değişiklikleri ve yeni Kurul kararları doğrultusunda günceller. Çalışanların Şirket politika ve prosedürlerine uygun hareket edip etmedikleri düzenli olarak denetlenir.
Siber Güvenlik Tedbirlerinin Alınması Maygold Petrol, elektronik ortamda işlenen kişisel verilerin güvenliğinin sağlanması amacıyla siber güvenlik önlemleri almaktadır. Bu kapsamda, hem şirket içi bilişim teknolojisi çalışanlarının hem de uzman hizmet tedarikçilerin yardımıyla Şirket, bir siber güvenlik zafiyetine uğranmaması adına gerekli tüm tedbirleri alır. Örneğin, **Anti-Virüs:** Maygold Petrol'in bilgi teknolojileri altyapısında bulunan tüm bilgisayar ve sunucularda periyodik olarak güncellenen lisanslı anti-virüs uygulaması yüklüdür. **Firewall:** Maygold Petrol, sunucularını barındıran Data Center ve Felaket Kurtarma Merkezleri periyodik olarak güncellenen yazılım yüklü firewall tarafından korunmakta olup, ilgili yeni nesil firewalllar tüm personellerin internet bağlantılarını kontrol etmekte ve bu kontrol sırasında virüs ve benzeri tehditlere karşı koruma sağlamaktadır. **DLP:** Verilerin, şirket içinde nasıl yer değiştirdiğini gözlemleyen ve kontrollü bir şekilde; "dışarı sızmalarını" engelleyen Veri Kaybı Önleme yazılımı kullanılmaktadır. **DRM:** Dijital dosyaların şirket içinde hangi koşullarda kullanılabileceği ve paylaşılabileceği hakkında düzenlemeler getiren Dijital Haklar Yönetimi (DRM) yazılımı kullanılmaktadır. **VPN:** Sunucu sistemlerine IP-SEC VPN ile bağlanılmakta olup, 2 nokta arasındaki trafik şifreli bir şekilde iletilmektedir. Tedarikçiler de Maygold Petrol, sunucu ya da sistemlerine Firewalllar üzerinde tanımlı bulunan SSL-VPN aracılığı ile erişim sağlayabilmektedirler. Her bir tedarikçi için ayrı SSL-VPN tanımı yapılmış olup, yapılan tanımlama ile tedarikçi sadece kullanması gereken ya da yetkilendirmesi yapılan sistemlere erişim sağlamaktadır.	

Kullanıcı Tanımlamaları ve Need to Know: Maygold Petrol, çalışanlarının Maygold Petrol sistemlerine olan yetkileri sadece iş tanımları ile gerekli olduğu ölçüde sınırlandırılmış olup, herhangi bir yetki ve görev değişikliği söz konusu olması durumunda sistemsel yetkileri de ivedi olarak güncellenmektedir.

Kişisel Veri Güvenliğinin Takibi

Maygold Petrol, hem fiziksel işlenen kişisel verilerin korunmasına ilişkin düzenli olarak denetim yapmaktadır. Örneğin, çalışanların "clean table & clean desk" prensibine uyup uymadığı, fiziksel ortamda bulunan kişisel veri içeren belgelerin kilit altına alınıp alınmadığı düzenli olarak yapılan ofis denetimlerinde kontrol edilmektedir.

Maygold Petrol, aynı zamanda elektronik ortamda işlenen kişisel verilerin güvenliğinin sağlanıp sağlanmadığına da ilişkin olarak testler yapmaktadır. Bu kapsamda özellikle koruyucu yazılım sistemlerinin çalışıp çalışmadığı, log kayıtları aracılığı ile elektronik yetkilendirmelerde usulüne uygun hareket edilip edilmediği gibi hususlar sürekli olarak denetlenmektedir. Söz konusu denetlemeler aşağıda örneklenen testler aracılığı ile de yapılmaktadır:

Fishing E-mail Testler: Maygold Petrol sistem kullanıcılarının farkındalığını artırmak için düzenli olarak kullanıcılara Fishing e-mailleri gönderilmektedir. Çıkan sonuçlara göre kullanıcılara Maygold Petrol Kullanıcı Portalı üzerinden eğitim tanımlanmaktadır.

Sızma Testi: Periyodik olarak Maygold Petrol sistemindeki sunuculara, bilgisayarlarına ve örnek bir mağazaya sızma testi manuel olarak tedarikçi bir firma tarafından yapılmaktadır. Bu test sonucunda oluşan güvenlik açıkları kapatılarak, ilgili güvenlik açıklarının kapatıldığına dair doğrulama testi yapılmaktadır. Ayrıca Bilgi Güvenliği Tehdit ve Olay Yönetimi sistemi tarafından da otomatik olarak sızma testi yapılmaktadır.

Bilgi Güvenliği Tehdit ve Olay Yönetimi: Maygold Petrol, sunucularında ve Firewall'larında oluşan olaylar "Bilgi Güvenliği Tehdit ve Olay Yönetimi" sistemine aktarılmaktadır. Bu sistem güvenlik tehdidi oluştuğunda sorumlu personelleri uyarmakta ve ivedi

Mevcut Risk ve Tehditlerin Belirlenmesi

Maygold Petrol, kişisel veri güvenliğini zafiyete uğratabilecek her türlü risk ve tehditleri, bir ihlal meydana gelmeden önce belirler. Bu kapsamda risk ve tehditlerin hangi veri kategorilerine, hangi işleme faaliyetlerine ve araçlarına ilişkin olduğu konusunda iç değerlendirme yapar. Söz konusu değerlendirme yapılırken, özellikle risk ve tehditlerin özel nitelikli kişisel verilere ilişkin olup olmadığına dikkat eder.

Maygold Petrol, belirlemiş olduğu risk ve tehditlerin minimize edilmesi, önlenmesi ve ortadan kaldırılması için gerekli adımları atar.

Çalışanlara Yönelik Önlemler

Maygold Petrol, çalışanlarının, çeşitli bilgi güvenliği ihlallerine karşı farkındalıklarını artırmak, kişisel verilerin hukuka uygun işlenmesi ve bilgi ihlali olaylarında insan faktörünün etkisini en aza indirmek amacıyla gerek Şirket içi departmanlarımızca, gerekse de hukuki ve teknik danışmanlık hizmeti aldığımız taraflarca eğitimler verilmektedir.

Maygold Petrol, çalışanlarını kişisel verilerin korunmasına ilişkin bilinçlenmeleri adına düzenli eğitim süreçleri, bilgilendirme yazıları, sözlü bilgilendirmeler ve iç yönergeler sunar. Bu kapsamda çalışanlar, kişisel verilerin toplanmasından imha edilmesi

bir şekilde tehdide cevap verilmesi imkanı sağlamaktadır.	sürecine kadar karşılaşacakları her işleme süreci hakkında detaylı yönergeler alırlar. Çalışanlara yönelik bilinçlendirme faaliyetleri kişisel verilerin korunmasına ilişkin güncel mevzuat değişiklikleri ve Kurul kararlarını da içerecek şekilde istihdam süresi boyunca devam eder. Çalışanlar iş sözleşmelerinde bulunan gizlilik yükümlülüklerine ek olarak, kişisel verilerin korunmasına ilişkin taahhütname de imzalarlar.
Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması Maygold Petrol, fiziksel ortamda muhafaza edilen kişisel verilerin güvenliğine ilişkin olarak özel güvenlik tedbirleri uygulamaktadır. Örneğin, - Kişisel veri muhafaza edilen fiziki ortamlar kilit altında tutulmaktadır. Bu kapsamda erişim yetkileri sınırlandırılmıştır. - Yangın, sel, hırsızlık gibi durumlara karşı gerekli önlemler alınmaktadır. - Kağıt yoluyla aktarılan kişisel veriler için ekstra önlemler alınmaktadır. Bu kapsamda kağıt yoluyla kişisel verilerin aktarılmasında, kapalı ve mühürlü zarf metodu kullanılmaktadır. - Sunucu veya arşiv odalarına giriş çıkışlar ek güvenlik tedbirleri ile korunmaktadır.	**Veri Minimizasyonu** Maygold Petrol, Kanun'un 4. maddesinde öngörülen ilkeler doğrultusunda, ilgili kişinin işleme faaliyeti kapsamında gerekli olmayan hiçbir verisini işlememeye özen gösterir. Bu noktada Şirket, işleme faaliyetini önceden inceler ve hukuki/ticari yükümlülüklerini yerine getirebilmesi için gerekli olan kişisel verileri ilgili kişiden talep eder. İlgili kişinin talep edilmeyen bir kişisel veri aktarması halinde bu kişisel veri derhal imha edilir veya maskelenir.
Kişisel Verilerin Yedeklenmesi Maygold Petrol, kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde yedeklenen kişisel verileri kullanarak kayıp riskini ortadan kaldırmaktadır. Yedeklenen kişisel verilerin güvenliği de en üst düzeyde sağlanmaktadır.	**Veri İşleyene Yönelik Tedbirler** Maygold Petrol, yürütmekte olduğu bir işleme faaliyetlerine ilişkin olarak alt-işleten desteği alacağı zaman öncelikle alt-işleyenin kişisel verilerin korunması konusundaki yetkinliğini ve yeterliliğini analiz eder. Bu kapsamda alt-işleyen asgari olarak Şirket'in öngörmüş olduğu kişisel verilerin korunması politikalarına ve prosedürlerine uygun hareket edeceğini yazılı bir şekilde taahhüt eder. Alt-işleyenin işleme faaliyetleri ve kişisel verileri korumasına yönelik çabaları Şirket tarafından denetlenir.

Diğer Örnekler

- Kişisel verilerin alındığı web sitesindeki tüm alanlar SSL ile korur.
- Birincil işleme amacı dışında kalan tüm ikincil veri işlemeler bakımından, Pseudonymization (takma adlı veri) yöntemini kullanır (Örnek: Ahmet Yılmaz → "A… Y…").
- Kağıt ortamdaki kişisel verilerin mutlaka kilitli dolaplarda muhafaza edilmesini ve sadece yetkili kişiler tarafından erişilmesini sağlar.
- Hizmet alınan üçüncü taraflara ait çerezler aracılığıyla işlenen kişisel veriler, üyelik sona erdiği takdirde üçüncü taraflara ait sistemlerden silinmektedir.
- Kapalı sistem ağ kullanılmakta olup, ağ ve yazılım güvenliği güncel ve lisanslı programlar ile veri kaybı önleme yazılımlarıyla korunmaktadır.
- Ağ ve yazılımlar üzerinde kullanıcı tanımlamaları ve yetki matrisleri mevcuttur.
- Yazılım sistemleri ve bulut depolama sistemleri çalışan yetkisine göre şifreli olarak kullanılmaktadır.
- Log kayıtları, kullanıcı müdahalesi olmayacak şekilde tutulmaktadır
- Gerektiği noktalarda veri maskeleme yöntemi kullanılmaktadır.

Özel Nitelikli Kişisel Verilere Özgü Tedbirler

Kurul'un 01/01/2018 Tarihli ve 2018/10 Sayılı Kararı gereği;

- Özel nitelikli kişisel verilerin işlenmesine yönelik olarak çalışanlara, periyodik eğitimler verilmektedir.
- Özel nitelikli kişisel verilerin işlendiği sözleşme süreçlerinde, özel nitelikli kişisel verilere özgü gizlilik sözleşmeleri ve taahhütnameleri imzalanmaktadır.
- Özel nitelikli kişisel verilere erişim yetkisine sahip çalışanların, yetki kapsamları ve süreleri net olarak tanımlanmıştır, bu yetkiler periyodik olarak denetlenmektedir.
- Özel nitelikli kişisel verilerin muhafaza edildiği elektronik ortamların kriptografik anahtarlarla, fiziksel ortamların ise anahtarlarının yetki matrislerine göre özel olarak temin edildiği kilitli ortamlarda güvenliği sağlanmaktadır.
- Log kayıtları düzenli olarak tutulmaktadır.
- Özel nitelikli kişisel verilerin bulunduğu yazılımlar sürekli olarak güncellenmektedir.
- Özel nitelikli kişisel verilere uzaktan erişim sağlanması gerekiyorsa, çift taraflı doğrulama anahtarları suretiyle erişim sağlanmaktadır.
- Özel nitelikli kişisel verilerin aktarımı elektronik ortamda, kriptografik yöntemlerle şifrelenmiş taşınabilir belleklerle, KEP adresiyle veya VPN kurularak veya sFTP yöntemiyle; fiziksel ortamlarda ise kişiye özel mühürlü ve zarflı belgeler ile aktarılmaktadır.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

Şirketimiz, kişisel verilerin saklanması ve imha edilmesi süreçlerinde yer alan kişileri, kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmekte

ve eğitilmektedir. Bu kapsamda, Şirketimiz çalışanları ve/veya görevleri dolayısıyla kişisel verileri öğrenen kişiler, bahse konu bilgileri Kanun ve diğer ilgili mevzuat hükümlerine uyun olarak saklamakta ve imha etmektedir. Bu yükümlülük, ilgili kişilerin görevden ayrılmalarından sonra da devam etmektedir.

Bu kapsamda, Şirketimizin saklama ve imha süreçlerinde yer alan kişilere ilişkin detaylar aşağıda açıklanmaktadır:

Unvan	**Birim**	**Görev**

9. SAKLAMA VE İMHA SÜRELERİ

Şirketimiz, kişisel verileri ancak ilgili uymakla yükümlü olduğu mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza ve imha etmektedir. Bu kapsamda Şirketimiz, kişisel verileri aşağıdaki EK-1 Saklama ve İmha Süreleri Tablosu'nda belirtilen azami süreler boyunca saklamakta ve imha etmektedir:

Kişisel veri sahibinin, Şirketimize başvurarak kendisine ait kişisel verilerin imha edilmesini talep etmesi halinde Şirketimiz:

(a) kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa:

(i) kişisel veri sahibinin talebini en geç otuz gün içinde sonuçlandırır ve kişisel veri sahibine bilgi verir, ve
(ii) talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa, bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde gerekli işlemlerin yapılmasını temin eder.

(b) kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, kişisel veri sahibinin talebini Kanun'un 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesini açıklayarak reddedilebilir ve ret cevabını kişisel veri sahibine en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

10. PERİYODİK İMHA SÜRELERİ

Şirketimiz, kişisel verileri imha etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri imha etmektedir. Bu kapsamda Şirketimiz, kişisel verileri imha etme yükümlülüğünün ortaya çıkması halinde kişisel verileri saklama süresinin sona ermesini takiben 6 ay içerisinde imha işlemine tabi tutmaktadır. Anılan süre, her hal ve koşulda Yönetmelik'in 11'inci maddesinde belirtilen azami periyodik imha süresini aşmamaktadır.

11. YÜRÜRLÜK

İşbu Politika [*Tarih Girilmelidir*] tarihinde yürürlüğe girmiştir. Politika değişen şartlara ve mevzuata uyum sağlamak amacıyla zaman zaman güncellenebilecektir. Güncel Politika [işbu platformda] yayımlandığı tarihte yürürlüğe girecektir.

İşbu Politika ile Kanun, Yönetmelik ve Maygold Petrol Kişisel Verilerin Korunması ve İşlenmesi Politikası hükümleri arasında herhangi bir çelişki olması halinde, Kanun, Yönetmelik ve Maygold Petrol Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda yer alan hükümler geçerli olacaktır.

EK – 1 Saklama ve İmha Süreleri Tablosu

Kişisel veriler, ilgili mevzuat veya Şirket uygulaması gereği daha uzun bir süre boyunca muhafaza edilmesi gerekmediği sürece, ortalama olarak aşağıdaki süreler doğrultusunda saklanacaktır.

Veri Tipi	Saklama Süresi	Hukuki Dayanağı	İmha Süresi
Çalışan Verileri	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	4857 Sayılı Kanun, 6098 Sayılı Kanun, 213 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanların Sağlık Verileri	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	4857 Sayılı Kanun, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşterilere İlişkin Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	6563 Sayılı Kanun, 6102 Sayılı Kanun, 6098 Sayılı Kanun, 213 Sayılı Kanun, 6502 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarikçilere İlişkin Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	6102 Sayılı Kanun, 6098 Sayılı Kanun ve 213 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Potansiyel Müşterilere/ Tedarikçilere İlişkin Kişisel Veriler	2 yıl	Veri Sorumlusunun Meşru Menfaati (Geriye ve İleriye Dönük Olarak Analiz Yapılması)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çevrimiçi Ziyaretçilere İlişkin Kişisel Veriler (Log Kayıtları)	2 yıl	5651 Sayılı Kanun ve ikincil mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Elektronik veya Basılı Ortamda Yayınlanan Materyallerde Yer Alan Kişisel Veriler	Süresiz	Veri Sorumlusunun Meşru Menfaati	-
Ticari Elektronik İleti Gönderimine İlişkin Kayıtlar	Ticari elektronik ileti onaylarına ilişkin kayıtlar, onayın geçersizlik tarihinden itibaren 3 yıl; ticari elektronik iletiye ilişkin diğer kayıtlar toplanma tarihinden itibaren 3 yıl	6563 Sayılı Kanun; Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Çağrı Merkezi Kayıtları	3 yıl	6563 Sayılı Kanun; Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçilere İlişkin Kişisel Veriler (Kamera Kayıtları)	30 gün	Veri Sorumlusunun Meşru Menfaati	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

EK – 2 Versiyon Takip Tablosu

VERSİYON TAKİP TABLOSU		
Versiyon No.	**Güncellenme Tarihi**	**Değişiklik Açıklaması**