

KVKK'YA UYUM REHBERİ

2020

KVKK Nedir?

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla 6698 sayılı, 7 Nisan 2016 tarihinde yayınlanarak yürürlüğe giren “**Kişisel Verilerin Korunması Kanunu**”nun kısaltılmışıdır.

Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

Bu kanun ile kişisel verilerin sınırsız biçimde ve gelişi güzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmaktadır.

Kanunda “**kişisel verileri işlenen gerçek kişiler**” ifadesi kullanıldığından, kişisel verileri işlenen tüzel kişiler bu Kanunun kapsamı dışında tutulmuştur.



KVKK ile İlgili Bazı Tanımlar

Açık Rıza

Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

Anonim Hale Getirme

Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

İlgili Kişi

Kişisel verisi işlenen gerçek kişiyi ifade eder.

Kişisel Veri

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.

Kişisel Verilerin İşlenmesi

Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.

Veri İşleyen

Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Veri Kayıt Sistemi

Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

Veri Sorumlusu

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Kişisel Veri Nedir ?

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu kapsamdaki kişilere ait; yerleşim yerleri, kimlik bilgileri, telefon görüşmeleri, mesaj bilgileri kişisel veri olarak kabul edilmektedir. Kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir. Buna göre;

- 1. Gerçek kişiye ilişkin olma:** Kişisel veri, gerçek kişiye ilişkin olup, tüzel kişilere ilişkin veriler kişisel verinin tanımının dışındadır. Dolayısıyla, bir şirketin ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin bilgiler (bir gerçek kişiyle ilişkilendirilebilecekleri durumlar haricinde) kişisel veri sayılmayacaktır.
- 2. Kişiyi belirli veya belirlenebilir kılması:** Kişisel veri, ilgili kişinin doğrudan kimliğini gösterebileceği gibi, o kişinin kimliğini doğrudan göstermemekle birlikte, herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm bilgileri de kapsar.
- 3. Her türlü bilgi:** Bu ifade son derece geniş olup, bir gerçek kişinin; adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.

Kanunda hangi bilgilerin kişisel veri olarak kabul edileceğine ilişkin sınırlı sayım yoluna gidilmediğinden, kapsamının genişletilmesi mümkündür. Önemli olan verinin kişi ile ilişkilendiriliyor olması ya da onu tanımlayabilmesidir.

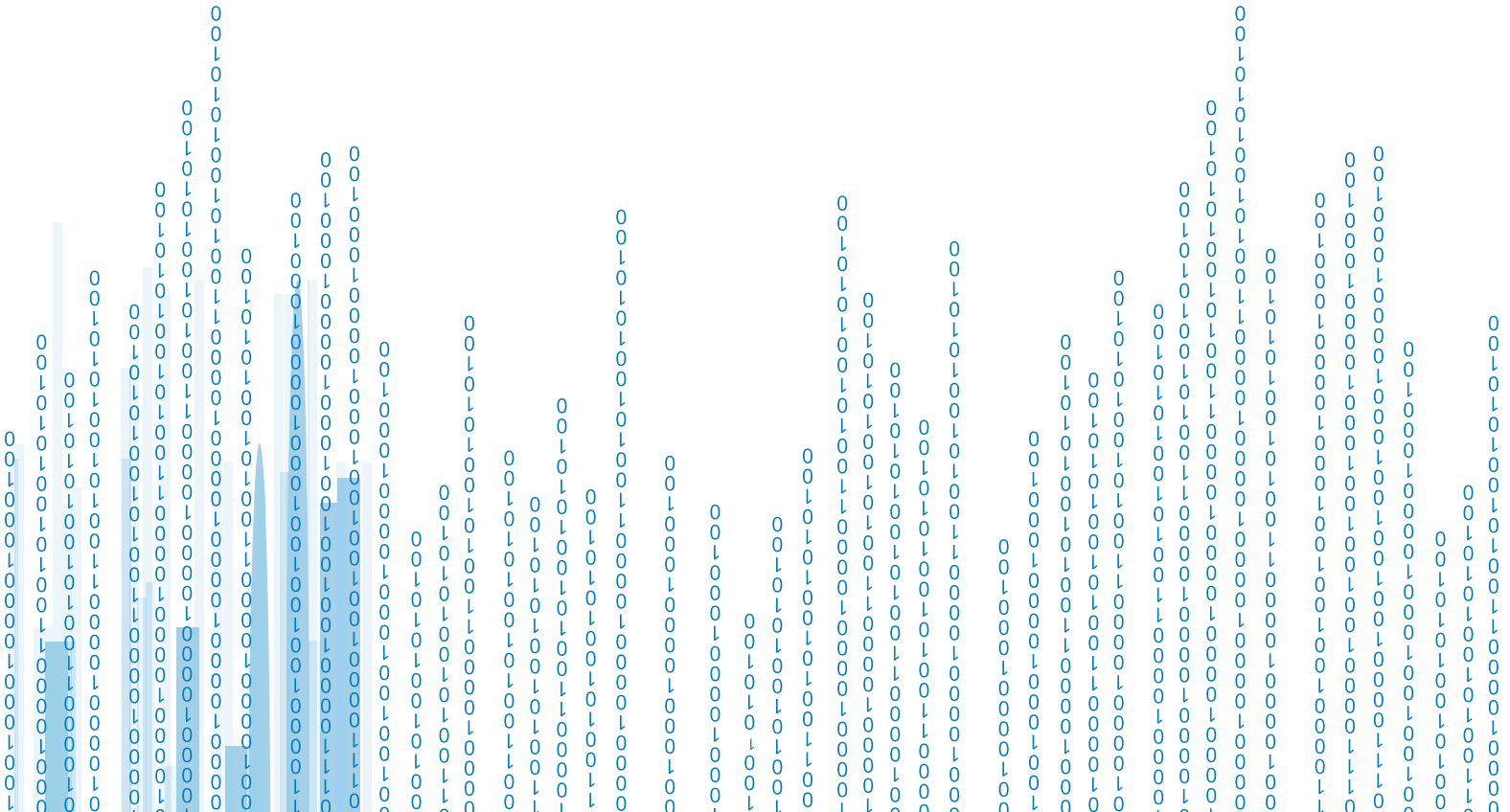
6698 sayılı Kanun m.6 uyarınca; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri kabul edilmekte ve bu verilerin, ilgilinin açık rızası olmaksızın işlenemeyeceği düzenlenmektedir.

Kişisel Verilerin İşlenmesinde Genel (Temel) İlkeler Nelerdir?

Uluslararası belgelerde kabul görmüş ve pek çok ülke uygulamasına yansımış olan kişisel verilerin işlenmesine ilişkin temel ilkeler bulunmaktadır. Kanunun 4. maddesinde kişisel verilerin işlenmesine ilişkin usul ve esaslar 108 sayılı Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine ve 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifine paralel şekilde düzenlenmiştir. Buna göre; Kanunda kişisel verilerin işlenmesinde sayılan genel ilkeler şunlardır:

- ✓ Hukuka ve dürüstlük kurallarına uygun olma,
- ✓ Doğru ve gerektiğinde güncel olma,
- ✓ Belirli, açık ve meşru amaçlar için işleme,
- ✓ İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- ✓ İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilmelidir.



Veri Sorumlusu Kimdir?

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizatihi kendileri "veri sorumlusu" olup, ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğacaktır. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemektedir.

Kanuna göre veri sorumlusu kişisel verilerin işleme amacını ve yöntemini belirleyen kişidir. Yani işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek kişidir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Ne Demektir?

Kişisel verilerin hukuka uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde bu veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

İşlenmesini gerektiren sebeplerin ortadan kalktığı hallerde kişisel verileri silmek, yok etmek veya anonim hale getirmek veri sorumlusunun yükümlülüklerindedir. Bunun için ilgili kişinin başvurusu şart değildir. Bununla birlikte, veri sorumlusunun ihmali durumunda ilgili kişinin kişisel verilerinin yok edilmesini veya silinmesini talep etme hakkı bulunmaktadır.

Öte yandan, Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik çerçevesinde kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, 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.

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

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, veri sorumlusu, 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 gerekir. Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Açık Rıza Alırken Dikkat Edilecek Hususlar Nelerdir?

Açık rıza; “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”dır. Kanun çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. Açık rızanın bir diğer önemi de veri işleyene gerçekleştireceği fiil konusunda yol göstermesidir. Kişi açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirmiş olmaktadır. Açık rıza, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme biçimini ve süresini de belirlemesini sağlayacaktır.

Açık rızanın bu anlamda, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerekmektedir. Diğer mevzuattaki düzenlemeler saklı kalmak üzere, açık rızanın yazılı şekilde alınmasına gerek yoktur. Açık rızanın elektronik ortam ve çağrı merkezi vb. yollarla alınması da mümkündür. Burada ispat yükümlülüğü veri sorumlusuna aittir. Kanunun 3. maddesinde yer verilen açık rıza tanımı kapsamında, açık rızanın 3 unsuru bulunmaktadır:

- Belirli bir konuya ilişkin olması,
- Rızanın bilgilendirmeye dayanması,
- Özgür iradeyle açıklanması.

Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar “battaniye rızalar” olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Örneğin; “her türlü ticari işlem, her türlü bankacılık işlemi ve her türlü veri işleme faaliyeti” gibi belirli bir konu ve faaliyeti işaret etmeyen rıza beyanları battaniye rıza kapsamında değerlendirilebilecek durumlardır.

Açık rıza vermek, kişiye sıkı sıkıya bağlı bir hak olduğundan, verilen açık rıza geri alınabilir. Bu bağlamda kişisel verilerin geleceğini belirleme hakkı ilgili kişiye ait olduğundan, kişi dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabilir.

Ancak, geri alma işlemi ileriye yönelik sonuç doğuracağından, açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetler geri alma beyanının veri sorumlusuna ulaştığı andan itibaren veri sorumlusu tarafından durdurulmalıdır. Bir diğer deyişle, geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğurur.

Veri Güvenliđi İin Yapılması Gerekenler

Veri Koruma

- Kritik veriler sistemde kontrol altına alınabilmeli
- İlgili kiřinin rızası bulunmuyorsa veri görülmemeli ve işlenmemeli
- Sadece görmesi gereken kişiler veriye ulaşmalı
- Verinin hem ekranda hem raporlarda kontrolü sağlanmalı
- Veri erişimi sistemdeki kullanıcıların yetkileriyle entegre olmalı
- Gerektiğinde veriler anonimleştirilebilmeli

Eriřim İzleme

- Kritik verilere erişim kayıt altına alınmalı
- Veriye erişim kayıtları istendiğinde raporlanabilmeli
- Bilgilendirme talepleri sistem tarafından takip edilip işlenebilmeli

KVKK Yaptırımları Nelerdir?

Hapis Cezası

- Kişisel verileri, belirli sürenin geçmesine karşın yok etmeme: 1-2 yıl
- Kişisel verileri hukuka aykırı olarak başkasına verme, yayma, ele geçirme: 2-4 yıl
- Kişisel verilerin hukuka aykırı olarak kaydedilmesi: 1-3 yıl

İdari Para Cezası

- Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırılık: 20.000 TL-1.000.000 TL
- Aydınlatma yükümlülüğünün ihlali: 5.000 TL-100.000 TL
- Veri güvenliği yükümlülüğünün ihlali: 15.000 TL-1.000.000 TL
- Kişisel Verileri Koruma Kurulu kararlarına muhalefet: 25.000 TL-1.000.000 TL

Kişisel Veri Yönetiminin Sağlanması

• Verilerin tekilleştirilmesi

Kişisel verinin işlenmesi süreciyle ilgili firma üzerindeki riskleri minimize etmek etmenin diğer bir adımı da veri kayıt ortamlarını minimize etmektir. İşlenen bir veri zorunlu olmadıkça tek bir kayıt ortamında bulunmalı ve bu kayıt ortamı da kontrol altında tutulmalıdır. DAM içerisindeki raporlar aracılığıyla belirlenen veri kayıt ortamlarının tekilleştirilmesi süreci yürütülmelidir. Bu tekilleştirme işlemi, tüm veri kayıt ortamlarının değerlendirilerek yeni bir sistem tasarımı oluşturulması ile sağlanmalıdır. Çalışma sonucunda en güvenli yapı verinin tek bir yerde kayıt altında tutulduğu yapı olacaktır. Bu süreçte dikkat edilmesi gereken diğer bir nokta ise, SAP ortamında bulunmayan verilerin de kontrollü bir ortama aktarılmasıdır. Özellikle kağıt ortamında tutulan verilerin kağıt ortamından elektronik ortama aktarılması denetim gücünü arttıracaktır. Böylece kağıt ortamdaki veriler imha edilip sistemdeki merkezi veri işleme noktasından bilgilere ulaşılabilir.

• Veri kütüphanesinin ve bilgi kümelerinin tanımlanması

DAM ile kişisel verilerin kontrol edilebilmesi için bilgi kümelerinin sisteme tanımlanması gereklidir. Bilgi kümeleri meşru amaçlar ile kişisel veri kataloğunda bulunan verilerin eşleştirildiği nesnelere dir. Bu nesnelere meşru amaca bağlı olarak hangi kişisel verilerin işlendiğini göstermektedir. DAM, hazır bir bilgi kümesi yapısı ile gelmektedir. Firma ise, kendi iş süreçlerine göre bu bilgi kümelerini güncelleyebilmektedir.

• Açık rızaların takibi

İşlenmesi kararlaştırılan kişisel veriler için ilgili kişilerden açık rızaların alınması ve bu açık rızaların takip edilmesi gereklidir. Bu amaçla DAM içerisindeki açık rıza modülü aracılığıyla ilgili kişilerden kişisel verileriyle ilgili rızaları talep edilir. İlgili kişilerin hangi kişisel verilere rıza verdiği sistemde takip edilmelidir. DAM veri tabanı alınan rızaların takibi için gerekli fonksiyonlara sahiptir. Rızalar elektronik ortamda toplanabileceği gibi, ıslak imzalı rızalar da sisteme taranarak yüklenmekte ve rıza takibi sağlanmaktadır.



Anonimleştirme

- Anonimleştirme taleplerinin alınması

Anonimleştirme taleplerinin kayıt altına alınması ve taleplerin cevaplanması veri sorumlusunun yükümlülükleri arasındadır. Bu süreci kontrollü yönetebilmek için DAM içinde bulunan anonimleştirme modülü kullanılabilir. Bu modül, gelen talepleri kaydetmekte ve yöneticiler için görev yaratmaktadır. Bu modül aracılığıyla yöneticiler gerekli aksiyonları planlayabilmektedirler.

- Anonimleştirme kayıt yönetimi

Anonimleştirme taleplerine cevap verilmesi bir yükümlülüktür. Cevabın olumlu olması durumunda ise, sistemlerde bulunan ilişkili veriler artık işlenemez. Bu verilere erişim de mümkün olmamalıdır. Bu sebeple kayıt altına alınmış ve onaylanmış anonimleştirme talepleri veri sorumlusu firmanın tüm sistemleri tarafından dikkate alınmalıdır. DAM, merkezi ortamda bu kontrolleri sağlamakta ve anonimleştirme işleminden sonra verileri gölgeleyerek SAP içinden verilere erişim imkanını kaldırmaktadır.



Raporlama

• Kullanım logları inceleme

Kişisel verilere erişimler ve verilerin dağıtımıyla ilgili kayıtlar sistemde güvenli olarak tutulmalıdır. Bu verilere erişen kişi ve sistemler kolaylıkla raporlanabilmelidir. Bu amaçla DAM, veri kataloğundaki verilere erişimleri izlemekte ve kayıt altına almaktadır.

• Muhatapların bilgilendirilmesi

İlgili kişilerin veya resmi kurumların talebine istinaden ilişkili kişisel verilerle ilgili bilgilendirme yapılması veri sorumlusunun yükümlülüklerindedir. Bu amaçla DAM, bilgilendirme taleplerini kayıt altına alan ve paylaşılan bilgilendirme yazıları ve raporlarını takip eden Bilgilendirme modülüne sahiptir. Bu modül ile talepler sistemde bir iş akışını tetiklemekte ve ön görülen sürelerde işlemlerin tamamlanması sağlanmaktadır.



Teknoloj Mimarı

NESİL BİLİŞİM Hakkında

2003'den Beri Sektördeyiz

Nesil Bilişim Teknolojileri A.Ş 15 yılı aşkın süredir uluslararası standartlarda, kaliteli,yenilikçi ve çözüm odaklı hizmet veren ve dünya pazarlarında 120'den fazla tedarikçi ile çalışmaktadır.

Kumu ve Özel sektörlerine hizmet veren firmamız, TSE ve ISO sertifikalarına sahip olmakla beraber bu standartlar çerçevesinde fark yaratmayı seven ve mükemmeliyetçi iş anlayışına sahip personelleri ile Profesyonel hizmet vermektedir.

Misyon

Bilgi ve iletişim teknolojilerinde yenilikçi çözümleri ile insan hayatına ve yaşam kalitesine değer katmaktır.

Vizyon

15 yıla dayanan tecrübesi, microsoft sertifikalı dinamik kadrosu ile ürün ve hizmet kalitesinde sektör liderliğini devam ettiren, alanında Türkiye'debilinen ve tercih edilen üç markasından biri olmaktadır.



Ankara Ofis Adres

Cevizlidere Mahallesi 1256. Cadde No: 10/A Balgat, Çankaya/Ankara

Telefon: 0850 532 08 96 - 0312 911 46 40

İstanbul Ofis Adres

Emniyetevleri Mahallesi, Yeniçeri Sokak Güler İş Merkezi No:2/3 Kağıthane/İstanbul

Telefon: 0212 975 00 97

E-Posta: ik@nesilteknoloji.com - kvkk@nesilteknoloji.com
