



# GSG Hukuk

## Aylık KVK Bülteni

### Şubat 2018

www.gsg hukuk.com

Bu sayıda

## Güncel Haberler:

### Kişisel Verileri Koruma Kurulu Kararları:

Kurul, 21 Aralık 2017 tarihli kararlarını geçtiğimiz günlerde yayınlamıştır.

Bu kararlardan ilkinde, ilgili kişilerin açık rızaları alınmaksızın, isim verilerinden telefon numarası verilerini elde etme veya telefon numarası verilerinden isim verilerinin sorgulanması şeklinde rehberlik hizmeti sunan internet siteleri ve uygulamalarına ilişkin olarak, bu faaliyetlerin bir veri işleme faaliyeti olduğunu ve bu uygulamaların KVKK m. 5'te belirtilen kişisel verilerin hukuka uygun işleme şartlarını yerine getirmediklerini belirtmiştir.

Bu kapsamda, veri işlemenin KVKK'ya aykırı olduğu gerekçesiyle ihlal kararı vermiştir. Kurul, KVKK m. 15/7 uyarınca telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık halinde verinin işlenmesinin durdurulmasına karar verme yetkisini kullanarak bu faaliyetler çerçevesinde hukuka aykırı olarak nitelendirilen veri işleme faaliyetlerinin derhal durdurulmasına hükmetmiştir.

GSG Hukuk

Faaliyetlerin durdurulmaması durumunda, internet sitelerine/uygulamalara erişimin engellenmesi için yetkili kurumlara başvurulacağı ve durumun Türk Ceza Kanunu'nun "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" başlıklı 136. maddesi uyarınca Cumhuriyet Başsavcılığına bildirileceğini belirtti. Kurul, bu kararın bir ilke karar teşkil ettiğini ve bu ilke karara uymayanlar hakkında KVKK'nın "Kabahatler" başlıklı 18. maddesi uyarınca işlem yapılacağını da belirtmektedir.

İkinci kararında ise bankacılık ve sağlık sektörü başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili hizmet veren kamu ve özel sektör kurum ve kuruluşlarının, KVKK'nın 12. maddesi uyarınca, banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirine yakın konumda hizmet alanların birbirlerine ait kişisel

## 1 Güncel Haberler

- *Kişisel Verileri Koruma Kurulu kararları*
- *Fransa Ulusal Bilişim ve Haklar Komisyonu kararı*
- *Veri Sorumluları Sicil Yönetmeliği*
- *Teknik ve İdari Önlemlere ilişkin rehber*
- *Bilişim güvenliğine ilişkin SPK Düzenlemesi*

## 2 Makaleler

- *Çevrimiçi profillemeye ve çevrimiçi davranışsal reklamlık*
- *Çalışanlardan alınacak açık rıza*

verilerin duymasını, görmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri alması gerektiğine karar vermiştir.

Kurul, bu kararın da bir ilke karar teşkil ettiğini ve bu ilke karara uyanlar hakkında KVKK'nın "Kabahatler" başlıklı 18. maddesi uyarınca işlem yapılacağını belirtmektedir.

### Fransa Ulusal Bilişim ve Haklar Komisyonu kararı

Fransa'da kurulu Genesis Industries Limited şirketi, içinde bir mikrofon ve bir kamera bulunan ve telefon ya da tablet ile bağlantılı bir uygulamayla birlikte çalışan oyuncaklar üretmektedir. Bu oyuncaklar, çocukların çeşitli sorularına uygulama vasıtasıyla internet üzerinden buldukları cevaplarla yanıt vermektedirler.

Şikayet üzerine Komisyon tarafından yapılan denetimler sonucunda, komisyon, oyuncaklara 9 metre uzaklıkta bulunan ve telefonunda Bluetooth bulunan her kişinin bir şifreye ihtiyaç duymaksızın ve çocukların veya oyuncakların sahiplerinin haberi olmaksızın oyuncaklara bağlanabildiğini, çocuk ve oyuncak arasında veya oyuncakın yakınında geçen konuşmaları dinleyebildiğini ve kaydedebildiğini tespit etmiştir.

Ayrıca şirketin, oyuncaklarla yapılan konuşmalardan çocuklar, çocukların aileleri ve arkadaşları hakkında birçok veri topladığını, oyuncakların kullanıcılarının bu verilerin toplandığından ve oyuncaklarla yapılan konuşmaların içeriklerinin Avrupa Birliği üyesi olmayan bir ülkede bulan bir servis sunucusuna aktarıldığından haberlerinin olmadığı tespit edilmiştir.

Fransa Ulusal Bilişim ve Haklar Komisyonu (CNIL), bu durumun Fransa Kişisel Verilerin Korunması Kanunu'nu birinci maddesinde GSG Hukuk

bulunan "bilişim teknolojilerinin insan kimliğini, haklarını, gizliliğini ve diğer bireysel ve kamusal özgürlüklerini ihlal etmeyeceği" yükümlülüğünü ihlal ettiğine karar vermiştir. Bu kapsamda oyuncakların işleyişinin 2 ay içerisinde mevzuatla uyumlu hale gelmesini istemiştir. Bununla birlikte Komisyon, yapılan bu uyarının bir yaptırım niteliği taşımadığını, 2 ay içerisinde mevzuatla uyumlu hale gelmesi durumunda başka bir yaptırım öngörülmeceğini belirtmiştir.

### Veri Sorumluları Sicili Yönetmeliği

Veri Sorumluları Sicili Hakkında Yönetmelik 30 Aralık 2017 tarihli ve 30286 sayılı Resmi Gazete'de yayımlanmış ve 1 Ocak 2018 tarihinde yürürlüğe girmiştir.

Yönetmelik'in ardından Kişisel Verileri Koruma Kurumu ("Kurum"), öncelikle Veri Sorumluları Sicili'ne ("Sicil") kayıt yükümlülüğüne getirilecek istisnalar hakkında Kişisel Verileri Koruma Kurulu ("Kurul") kararının yayımlanması, hazırlanmakta olan Veri Sorumluları Sicili Bilgi Sisteminin (VERBİS) hizmete açılması ve Sicil'e kayıtlı ilgili olarak Kurul tarafından bir başlangıç tarihi belirlenerek kamuya duyurulması gerekeceğini belirtmiştir. Sicil'e kayıt yükümlülüğünün, ancak bu işlemlerin tamamlanmasından sonra başlayacaktır.

Bu sebeple halihazırda Veri Sorumlularının Sicil'e kayıt yükümlülüğü uygulanmamaktadır.

### Teknik ve İdari Önlemlere İlişkin Rehber

Kurum, KVKK m. 12 çerçevesinde alınması gereken teknik ve idari tedbirlere ilişkin merakla beklenen rehberi yayınladı. Kişisel veri güvenliğine ilişkin idari tedbirler yanda açıklanmaktadır:

**Mevcut risk ve tehditlerin belirlenmesi:** Rehber'e göre bu riskler belirlenirken veri sorumlusu tarafından kişisel verilerin özel nitelikli veri olup olmadığı, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği ve güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

### Çalışanların eğitilmesi ve farkındalık çalışmalarının yürütülmesi:

Rehber' göre siber güvenliğin sağlanması, kişisel verilerin hukuka aykırı olarak açıklanması veya paylaşılmasının engellenmesi amacıyla çalışanların eğitilmesi ve gerekli hallerde ilk müdahaleyi yapmaları büyük önem taşımaktadır. Erişim yönetimi açısından ise kurum kültürü oluşturulurken "yasaklanmadıkça her şey serbesttir" prensibi değil "izin verilmedikçe her şey yasaktır" prensibinin temel alınması gerektiği vurgulanmıştır. Öte yandan çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşması imzalamaları istenebileceği seçenek olarak belirtilmiş, çalışanların veri güvenliği politika ve prosedürlerine uymaması durumunda ise bir disiplin süreci planlanması zorunlu tutulmuştur.

### Kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi:

Belirlenen politika ve prosedürlere ilişkin olarak; veri sorumlusu tarafından kontrollerin düzenli olarak yapılması, belgelenmesi, geliştirilmesi gereken hususların tespit edilmesi ve gerekli hallerde güncellemeler yapılması önerilmiştir. Ayrıca, politika ve prosedürlerde her nevi kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceğinin de açıkça belirlenmesi gerektiği vurgulanmıştır.

**Kişisel verilerin mümkün olduğunca azaltılması:** Özellikle uzun süredir faaliyet gösteren veri sorumluları çok fazla miktarda kişisel veri toplamakta ve bu veriler uzun süre sonucunda bir amaca hizmet etmeyen ve güncelliğini yitirmiş veriler haline gelebilmektedir. Bu nedenle kişisel verilerin güncelliğinin düzenli aralıklarla kontrol edilmesi, ihtiyaç duyulmayan kişisel verilerin ise oluşturulan saklama ve imha politikası kapsamında güvenli bir şekilde imha edilmesi gerekmektedir.

### **Veri işleyenler ile ilişkilerin yönetilmesi:**

KVKK'nın 12. maddesine göre veri işleyenler de veri sorumluları ile birlikte veri güvenliğinin sağlanmasında müştereken sorumlu olacaktırlar. Ayrıca sır saklama yükümlülüğü ve veri sorumlusunun veri işleyen üzerindeki denetim yükümlülüğü de ilgili sözleşmede düzenlenmelidir.

Kişisel veri güvenliğine ilişkin **teknik tedbirler** kapsamında ise, siber güvenliğin sağlanması amacıyla güvenlik duvarı ve ağ geçidi gibi sistemlerin kurularak internet üzerinden gelebilecek olası saldırıların önüne geçilmesi önerilmiştir. Öte yandan, erişim yönetimi açısından ise veri sorumlularına bu hususa ilişkin ayrı bir politika/prosedür ve erişim yetki ve kontrol matrisi oluşturmaları ve çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanımları ve ilgili sistemlere kullanıcı adı ve şifre kullanılmak suretiyle erişim sağlanması tavsiye edilmiştir.

### **Bilişim Güvenliğine İlişkin SPK Düzenlemesi**

5 Ocak 2018 tarihli 30292 sayılı Resmi Gazete'de yayımlanarak

yürürlüğe giren Bilgi Sistemleri Yönetimi Tebliği ile Borsa İstanbul A.Ş., borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri, emeklilik yatırım fonları, İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., portföy saklayıcısı kuruluşlar, Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş., sermaye piyasası kurumları, halka açık ortaklıklar, Türkiye Sermaye Piyasaları Birliği ve Türkiye Değerleme Uzmanları Birliği olmak üzere tebliğde yer alan kurum, kuruluş ve ortaklıklara veri gizliliğine ilişkin yeni yükümlülükler getirilmiştir.

Söz konusu tebliğinin Veri Gizliliği başlıklı 17. Maddesi uyarınca; *Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır.* (...)

Söz konusu tebliğin Bilgi Sistemlerine İlişkin Dış Kaynak Yoluyla Alınan Hizmetlerin Yönetimi başlıklı 18. maddesi aşağıdaki şekildedir: *Kurum, Kuruluş ve Ortaklıkların üst yönetimi tarafından, bilgi sistemleri kapsamında dış kaynak yoluyla alınacak hizmetlerin doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak bir gözetim mekanizması tesis edilir. Tesis edilecek gözetim mekanizması asgari olarak aşağıda belirtilen hususları içerir:* (...)

b) *Kurum, Kuruluş ve Ortaklıkların verilerinin dış kaynak yoluyla alınan bilgi*

*sistemleri hizmeti sağlayan kuruluşa aktarılmasının gerekli olduğu durumlarda, söz konusu kuruluşun bilgi güvenliği konusundaki ilke ve uygulamalarının en az Kurum, Kuruluş ve Ortaklıkların uyguladığı düzeyde olması, (...)*

Söz konusu tebliğin Müşteri Bilgilerinin Gizliliği başlıklı 19. Maddesi aşağıdaki şekildedir: *Kurum, Kuruluş ve Ortaklıklar bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin gizliliğini sağlamaya yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır.*

*Kurum, Kuruluş ve Ortaklıklar personelin kişisel verilerin korunması ve işlenmesine uygun davranışlarını temin etmelerine yönelik gerekli tedbirleri alırlar. Bu maddede yer almayan durumlarda 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uygulanır.*

Ayrıca yine 5 Ocak 2018 tarihli 30292 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bilgi Sistemleri Bağımsız Denetim Tebliği ile Borsa İstanbul A.Ş., borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri, emeklilik yatırım fonları, İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., portföy saklayıcısı kuruluşlar, Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş., sermaye piyasası kurumları, halka açık ortaklıklar, Türkiye Sermaye Piyasaları Birliği ve Türkiye Değerleme Uzmanları Birliği olmak üzere aynı kurum, kuruluş ve ortaklıklara veri gizliliği ve bilgi güvenliği kapsamında ek yükümlülükler getirilmiştir.



## KVK Makaleleri:

### Çevrimiçi Profillemeye ve Çevrimiçi Davranışsal Reklamcılık

Kişisel verilerin korunması hukuku Avrupa’da uzun bir süredir var olmakla birlikte 95/46 Direktifi - bazı konseptler (özellikle teknolojik gelişmeler) açısından yeterince net bir düzenleme olarak değerlendirilmeyordu. Örneğin, İnternet Protokolleri (IP adresleri) ve çerezler aracılığıyla ilgili kişilerin çevrimiçi profillerinin oluşturulması ve bu kapsamda davranışsal reklamcılık faaliyetlerinde bulunulması, IP adreslerinin ve çerezlerin kişisel veri olarak değerlendirilip değerlendirilemeyeceği tartışmalarını gündeme getirmekteydi.

Genel Veri Koruma Yönetmeliği (“GDPR”) ile birlikte kişisel veri, “gerçek bir kişinin kimliğini belirleyen veya belirlenebilir kulan her türlü bilgi” olarak tanımlandı. GDPR bunun yanında bir kişiyi belirlenebilir kılmanın, doğrudan veya dolaylı olarak, özellikle bir isim, kimlik numarası, yer bilgisi, çevrimiçi tanımlayıcı, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimlik veya fiziksel, fizyolojik özelliklere özgü bir veya daha fazla faktör ile belirlenebilir kılınması olarak ifade etmektedir. Bu tanımda yeni yer verilen kavramlardan biri olan çevrimiçi tanımlayıcıları, IP adresleri ve çerezlerin GDPR ile birlikte kişisel verinin kapsamının günümüz teknolojik gelişmelerine paralel olarak genişlediği söylenebilir.

KVKK ise IP adresleri ve çerezlerin kişisel veri olup olmadığı ve bu teknolojik araçların şirketler tarafından kullanılarak çevrimiçi reklamcılık faaliyetlerinde bulunması konusunda sessiz kalmaktadır.

Çevrimiçi Davranışsal Reklamcılık

farklı metotlarla yapılabilmektedir. Bunlardan ilki, reklam ağlarının birinci (Veri Sorumlusu’nun kendi sitesi üzerinden) veya üçüncü taraf izleme etkinlikleri ile yayıncıların reklam ağları ile iş birliği içinde yapılmasıdır (bu hizmetleri veren şirketler vasıtasıyla). Teknik detayları olan ve İnternet servis sağlayıcıları tarafından kullanılan “Derin Paket Analizi” (Deep Package Inspection) olarak bilinen yöntem de bir başka çevrimiçi davranışsal reklamcılık faaliyeti metodu olarak örnek gösterilebilir.

Her iki yöntemde de ortak olan tarayıcı çerezleri ve bunlar aracılığıyla IP adreslerinin takibi ile kullanıcı profillemeye teknikleri kullanılmakta ve kullanıcılara ilgi alanları doğrultusunda reklam gösterme amaçlanmaktadır. Bu reklam modelinde kişiye özel reklam amaçlandığından dolayı bu faaliyet sırasında çerezler ve IP adresleri aracılığıyla kişisel veriler işlenmekte, onların İnternet ağı üzerinden tutum ve davranışları ile İnternet alışkanlıkları kaydedilmekte ve bunun sonucu olarak ilgili kişi özelinde çevrimiçi reklam faaliyetlerinde bulunulmaktadır.

Bu reklam modelini hedefleyen ve kullanan şirketler Veri Sorumlusu olacaktır. Bu modelle işlenen kişisel verilerin KVKK’ya uygun olarak aydınlatma yapılması ve açık rıza alınması suretiyle işlenmesi gerekecektir. Bu açık rıza alma ve aydınlatma metinleri İnternet ortamından alınmasında herhangi bir hukuki engel yoktur. Bunun yanında Veri Sorumlularının davranışsal reklamcılık faaliyetlerini kendileri yürütmek yerine bir hizmet sağlayıcı vasıtasıyla yürütmeleri de mümkündür. Bu durumda Veri

Sorumlusu – Veri İşleyen ilişkisi analiz edilmeli, KVKK kapsamında aydınlatma ve açık rıza yükümlülüklerinin kim tarafından yerine getirileceği belirlenmelidir. Özellikle e-ticaret ya da perakende şirketleri açısından davranışsal reklamcılık faaliyetleri kapsamında işlenen kişisel verilerin KVKK, Kurul ilke kararları ile rehberleri ve Avrupa Birliği uygulamaları çerçevesinde şekillendirilmesi önemlidir.



## KVK Yazıları:

### Alınacak Açık Rıza

İşverenler -geçmiş, mevcut ve potansiyel- çalışanlarının kişisel verilerini işe alım, özlük dosyaları, ücret ödemeleri, hasta raporları, gözetleme faaliyetleri, performans değerlendirmeleri, işten ayrılma süreçleri gibi birçok farklı amaçla işlemektedirler.

İşverenler, bu kişisel verileri işlerken İş Hukuku'ndan kaynaklı yükümlülüklerini de yerine getirmektedirler. Öte taraftan, çalışanların kişisel verilerinin işverenler tarafından birçok farklı amaçla işlenmesi, çalışanların özel hayatının gizliliği başta olmak üzere, temel hak ve özgürlükleri konusunda bir takım sakıncalar doğurmaktadır.

KVKK'nın yürürlüğe girmesiyle birlikte, ülkemizde yer alan her gerçek kişi gibi çalışanların kişisel verileri de kapsamlı bir korumaya sahip olmuştur. KVKK'nın yürürlüğe girmesi, işverenlerin bundan sonra çalışanlarının kişisel verilerini işleyemeyeceği anlamına gelmemektedir. Nitekim KVKK'nın amacı kişisel verilerin işlenmesini yasaklamak değil, bir düzenlemeye oturtmaktır. KVKK işverenlere, aradığı şartların sağlanması durumunda, çalışanlarının kişisel verilerini işleme olanağı tanımaktadır.

KVKK, kişisel veri işleme faaliyetini hukuka ve dürüstlük kurallarına uygun olmasını, işlenen kişisel verilerin doğru ve gerektiğinde güncel olmasını, belirli, açık ve meşru amaçlar için işlenmesini, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasını ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesini zorunlu kılmıştır.

İşverenler KVKK'nın 5. maddesinde yer alan şartlardan birine dayanarak çalışanların kişisel verilerini işleyebilecektir. Bu şartlardan biri de çalışanların kişisel verilerinin işlenmesi için açık rızanın alınmasıdır. İlk bakışta her ne kadar çalışanlardan açık rızanın alınması diğer şartlara nazaran daha kolay gözükse de aslında uygulamada bazı pratik sorunlar doğabilmekte, zaman zaman çalışan açık rıza vermekten kaçınabilmekte zaman zaman da açık rıza alınabilmesi için gerekli şartlar oluşmamaktadır.

KVKK kapsamında geçerli bir açık rızanın alınması için, bu rızanın özgür iradeye dayanması, belirli bir konuya veya amaca ilişkin olması, çalışanların kendisinden alınan kişisel verilere ilişkin bilgilendirilmiş olması ve alınan açık rızanın tereddütte yer bırakmayacak açıklıkta olması gerekmektedir. Bu anlamda, işverence çalışanlardan alınan açık rızanın belirtilen şartları taşıması ayrıca çalışanlara her zaman verdiği açık rızayı geri alabilme şansının tanınması gerekir. Ayrıca çalışanların geri alabileceği bu açık rızanın sonucu olarak kendisi için herhangi bir olumsuz sonucun doğmaması gerekir.

Bu konuda, Avrupa uygulamalarına baktığımızda, genel olarak her ülkenin veri koruma kurullarının ortak paydada bulunduğu nokta, çalışan ve işveren arasında güç dengesinde büyük eşitsizlik olması durumunda açık rızanın özgür iradeye dayalı olmasının mümkün olmadığı kabul edilmektedir. Ayrıca Avrupa'da Mayıs 2018 yılında yürürlüğe girecek olan GDPR gerekçesinin 43. paragrafında da çalışan ve işveren arasındaki güç

dengesizliğinin fazla olması durumunda, işverence çalışanın kişisel verilerinin işlenmesi için çalışanlardan alınan açık rıza sırasında çalışanların bu konuda baskı hissetmesi işveren ve çalışan arasındaki iş ilişkisinin niteliğiyle ilgilidir. Bu kapsamda özgür iradeden bahsedilemeyeceği belirtilmektedir.

İşverenler açısından KVKK'nın 5. maddesinde birtakım istisnalar getirmekte ve bu istisnalara dayanarak bir kısım kişisel veriler işlenebilmektedir. Bu nedenle istisna oluşturan durumlarda istisna hükümlerinin kullanılması ve istisna kapsamına girmeyen durumlarda kişisel verilerin işlenebilmesi için açık rıza alma yoluna gidilmesi daha isabetli olacaktır.

# GSG Hukuk

## Aylık Kişisel Verilerin Korunması Hukuku Bülteni

Şubat 2018

www.gsg hukuk.com



*KVKK kapsamında yerine  
getirmeniz gereken hukuki  
yükümlülükler hakkında  
daha detaylı bilgi almak için  
bizimle iletişime geçin*

Süleyman Seba Cad.  
No :48 BJK Plaza  
B Blok K:4 Akaretler  
Beşiktaş - İstanbul

+90 212 326 68 68

+90 212 326 68 69

info@gsg hukuk.com

**Nilgün Serdar Şimşek, LL.M.**

Ortak, Avukat

T: +90 (212) 326 63 68

nilgun.simsek@gsg hukuk.com

**Rıza Eroğlu**

Kıdemli Müdür

T: +90 (212) 326 64 61

riza.eroglu@gsg hukuk.com

**İpek Okucu Taftalı**

Kıdemli Avukat

T: +90 (212) 326 60 60/3881

ipek.okucu@gsg hukuk.com