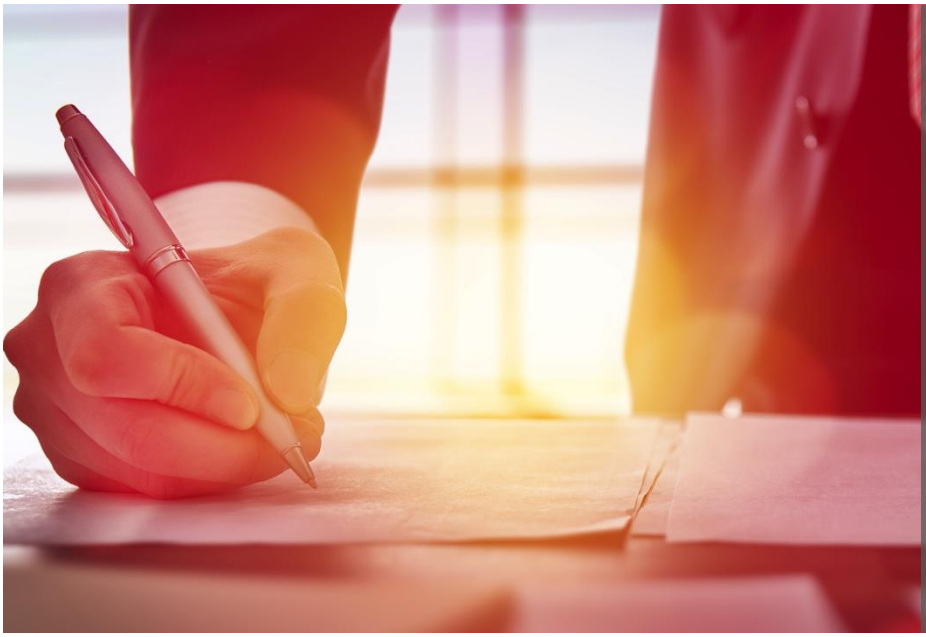

GSG Hukuk

Aylık KVK Bülteni

Nisan 2018

Bu sayıda

1 *Güncel Haberler*

2 *Makaleler*

Güncel Haberler:

Özel Nitelikli Kişisel Verilerin İşlenmesi ile ilgili Kurul Kararı yayınlandı

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler konulu ve 31 Ocak 2018 tarihli Kurul Kararı 7 Mart 2018 tarihli Resmi Gazete'de yayınlanmıştır. Söz konusu kararda Kurul, KVKK m. 6/4'te yer alan "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır*" hükmüne dayanarak özel nitelikli kişisel verilerin işlenmesi sırasında KVKK'da belirtilmeyen fakat alınması gereken önlemlere yer vermiştir.

Söz konusu karar ilerleyen sayfalarda yer alan "*Özel Nitelikli Kişisel Veriler Nasıl İşlenmeli ve Korunmalıdır?*" isimli makalede ayrıntılı olarak incelenmiştir.

Aydınlatma Yükümlülüğü ile ilgili Tebliğ Yürürlüğe girdi

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, 10 Mart 2018 tarihinde 30356 sayılı Resmi Gazete'de yayımlandı. Yayım tarihi ile beraber yürürlüğe giren Tebliğ, veri sorumlularının KVKK kapsamında yerine getirmeleri gereken aydınlatma yükümlülüklerine ilişkin usul ve esasları detaylandırmaktadır.

Söz konusu tebliğ, ilerleyen sayfalardaki "*Aydınlatma Yükümlülüğü Tebliği'nin Getirdiği Düzenlemeler*" isimli makalede ayrıntılı olarak incelenmiştir.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ Yürürlüğe girdi

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, 10 Mart 2018 tarihinde 30356 sayılı Resmi Gazete'de yayımlandı. Bu tebliğ, KVKK m. 13/1 ve m. 22/1 esas alınarak hazırlanmış olup veri sorumlularına başvuru hakkını, başvuru usulünü, başvuruya cevap ve başvuru ücretini düzenlemektedir.

Bilgi Sistemleri Düzenlemesi ile ilgili Sermaye Piyasası Kurulu Karar verdi

SPK'nın VII-128.9 sayılı "Bilgi Sistemleri Yönetimi Tebliği" ("**BSY**") ile III-62.2 sayılı "Bilgi Sistemleri Bağımsız Denetim Tebliği" ("**BSD**") 5 Ocak 2018 tarihli ve 30292 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmişti. Bu düzenlemeler ile sermaye piyasası mevzuatına tabi ortaklıkların birincil sistemlerini Türkiye'de tutmaları öngörülmekteydi.

Sermaye Piyasası Kurulu i-SPK.62.1 (01.03.2018 tarihli ve 9/327 s.k.) sayılı bir ilke karar vermiş ve 8 Mart 2018 tarihinde yayınladığı 2018/10 sayılı bülteninde bu kararını aşağıdaki şekilde duyurmuştur:

"*BSY'nin 28/3 ve BSD'nin 30/5 maddeleri uyarınca, Kurulumuz BSY ve BSD'de yer alan muafiyetleri kısmen ve tamamen kaldırmaya, bunların içeriğini kurum, kuruluş ve ortaklık bazında değiştirmeye yetkilidir.*

Bu kapsamda; BSD hükümleri kapsamında, bilgi sistemleri bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıkların BSY'nin 26/1 maddesi uyarınca, bu aşamada birincil sistemlerini yurtiçinde bulundurma zorunlulukları bulunmamaktadır. Ancak, BSD'nin 30/5 maddesinin Kurulumuza verdiği yetkiye istinaden bilgi sistemleri bağımsız denetim kapsamına girecek kurum, kuruluş ve ortaklıkların tedrici olarak genişletilmesi planlanmaktadır. Halka açık ortaklıklar, bilgi sistemleri bağımsız denetimine tabi olacakları dönem itibarıyla, BSY'nin 26/1 maddesi uyarınca birincil sistemlerini yurtiçinde tutmak zorunda olacaklardır".

Kurul tarafından 30.000 TL idari para cezası verildi

Tüketici mahkemesinde görülen spor salonu üyeliğinin sona erdirilmesi kaynaklı uyuşmazlıkta, mahkeme, spor salonu ücretinin iadesine ilişkin bankadan bilgi talep etmiştir. Banka ise yalnızca ücret iadesine ilişkin bilgi vermek yerine spor salonuna üye olan davalının 6 aylık kredi kartı ekstresini mahkemeye yollamış ve davalıya ilişkin kredi kartı ekstreleri dava dosyasına girmiştir.
Dava dosyasına erişimin avukat ve stajyer avukatlar tarafından mümkün olduğu göz önünde bulundurulduğunda davalıya ait kişisel verilerin birçok kişinin erişimine açılması ve veri sahibinin açık rızası alınmaksızın kişisel verilerin işlenmesi sebebiyle Kurul, 2018/13 sayılı ve 8 Şubat 2018 tarihli kararında KVKK m. 18/1/(b) uyarınca ilgili bankayı 30.000 TL idari para cezasına mahkum etmiştir.

Güncel Haberler:

Banka, Kurum'a ilettiği cevabında KVKK'ya uyum süreci kapsamında bilgi sistemlerinde gerekli altyapı ve yazılım çalışmalarının devam ettiğini ve personelin eğitimi yönünde çalışmalar yaptığını bildirmiştir. Bu doğrultuda Kurul, banka hakkında idari para cezası dışında ilave işlem yapılmasına gerek olmadığı yönünde karar almıştır.

Facebook'un Hisseleri uygunsuz Kişisel Veri Paylaşımı sebebiyle büyük değer kaybetti

İngiltere'de bir akademisyen kişilik testi içeren bir Facebook uygulaması geliştirmiş ve politik veri danışmanlığı şirketi olan Cambridge Analytica bu testin çözülmesi ve reklamının yapılması için finansman sağlamıştır. Bu uygulama ile her test sonunda testi çözen kişinin Facebook hesabındaki birtakım veriler kaydedilmiştir. Kaydedilen veriler yalnızca testi çözen kişi ile sınırlı kalmamış aynı zamanda bu kişinin Facebook arkadaşlarının bazı kişisel verileri de kayıt altına alarak belirli bir algoritma ve model oluşturmak amacıyla kullanılmıştır. Nitekim Facebook'un olağan ayarları – bu ayarlar kullanıcının kendisi tarafından değiştirilmedikçe - kullanıcıların arkadaşlarının verilerinin bu tarz uygulamalar tarafından toplanmasına izin vermektedir. Bu algoritma ve model daha sonra politik amaçlarla, oy kullanan kişilerin tercih ve özelliklerini belirlemek amacıyla izinsiz bir biçimde Cambridge Analytica tarafından kullanılmıştır. Bu kişisel veriler, ticari amaçla kullanılacağına ilişkin ilgili kişilerden ya da bu kişilerin Facebook arkadaşlarından hiçbir rıza almaksızın kaydedilmiştir. Facebook'un söz konusu akademisyene verdiği izin bu kişisel verilerin yalnızca akademik amaçlarla işlenmesi iken; akademisyen bu verileri Cambridge Analytica'nın politik pazarlama faaliyetleri için erişilebilir hale getirmiştir. Facebook Cambridge Analytica ile izinsiz veri paylaşımı yaptığı iddialarını kabul etmemiş ve veri ihlallerinin önüne geçmek için bu tür uygulamalara karşı güvenliğini arttıracağına ilişkin bir duyuru yayınlamıştır.

Facebook'un hisseleri, 50 milyona yakın kullanıcının verilerini Cambridge Analytica ile paylaştığı ifşa olduktan sonra oldukça fazla değer kaybetmiştir. Hisselerin değeri pazartesi günü akşama saatlerinde neredeyse %7 oranında düşerek Facebook'un 5 yılı aşkın süredir bir gün içerisinde düşmediği seviyeye düşmüştür.

İngiltere Veri Koruma Otoritesi bir firma çalışanına ceza verdi

Bir kaza onarım şirketi olan Nationwide Accident Repair Services Limited (NARS), birçok müşterinin kendilerinden hizmet almaya başladıktan kısa bir süre sonra, yaptıkları kazalar hakkında pazarlama amaçlı defalarca kez arandığını ve hukuki bir takipte bulunmak isteyip istemediklerinin sorulduğunu öğrenmesi üzerine siber güvenlik danışmanlarından destek isteyerek bir inceleme başlattı. Bu kapsamda NARS çalışanı 33 yaşındaki Phillip Bagnall'ın iş saatleri dışında evdeki bilgisayarında şüpheli bir yoğunlukta müşteri verisine ulaştığı tespit edildi.

Yapılan inceleme sonucunda Phillip Bagnall'ın işvereninin rızası olmaksızın 2.724 müşteri verisine eriştiği ortaya çıktı. Bu bulgunun ortaya çıkması ile birlikte NARS Phillip Bagnall'ı İngiltere Veri Koruma Ofisi ICO'ya şikayet etti. Konu daha sonra mahkemeye intikal ettirilerek, Phillip Bagnall 500 Euro para cezasına ek olarak, zararlar için 364 Euro ve mağdurlar için 50 Euro para cezasına çarptırıldı.

KVK Makaleleri: Olay Müdahalesinin Kişisel Veri Güvenliğindeki Rolü

Avrupa Birliği'ndeki yeni veri koruma mevzuatı olarak Mayıs 2018'de yürürlüğe girecek olan GDPR m. 5 uyarınca kişisel verilerin işlenmesi sırasında, kişisel verilerin güvenliği uygun teknik ve organizasyon yöntemler ile sağlanmalıdır. Kişisel verilerin güvenliğinin sağlanması, kişisel verilerin güvenliğini tehlikeye düşürebilecek olayların tespit edilmesi, ihlallerin ortaya çıkarılması ve bunlara müdahale edilmesini de kapsayan geniş bir kavram olup tüm bu süreçler "olay müdahalesi" olarak adlandırılmaktadır. GDPR'ın Gerekçesi m. 49'da da kişisel verilerin güvenliğinin sağlanması bakımından olay müdahalesine değinilmiştir.

Olay müdahalesi için belirli birtakım kıstasları sağlayan bir olay müdahalesi planının varlığı gereklidir. Olay müdahalesi planı genel itibariyle, kıdemli yöneticilerin onayı ile olay müdahalesinin ileriye yönelik tutumunu, müdahalenin şeklini ve yöntemini içeren idari bir modeldir. Bu kapsamda her organizasyon kendisine uygun olan olay müdahalesi yöntemini seçmeli ve bu yönteme uygun bir olay müdahalesi planı oluşturmalıdır. Uygun bir olay müdahalesi planı, olay müdahalesi sürecinde nasıl, ne zaman ve neden karar alınacağını; bu kararların alınma amacının farkında olan kişileri ve bu kişilerin görev dağılımlarını içeren bir olay müdahalesi ekibi listesi içermelidir. Olay müdahalesi planının devamlı güncellenmesi ve yürürlükteki hukuki düzenlemelere uygun ilerlemesi gerekmektedir.

Olay müdahalesinin önemi, GDPR m. 33 ile birlikte değerlendirilmelidir. GDPR m. 33 kişisel veri ihlallerin bildirilmesini düzenlemekte ve ihlalin öğrenilmesinden itibaren 72 saatlik bir bildirim süresi öngörmektedir. Olay müdahalesinde özellikle alışılmışın dışında olayların söz konusu süre içinde raporlanması ve bu raporlama için gerekli teknik altyapının sağlanması bir zorunluluktur. Zira aksi takdirde kişisel veri güvenliğini tehlikeye düşürebilecek olaylar tespit edilemeyeceğinden müdahale söz konusu olmayacak ve olaylar kişisel veri güvenliğinin ihlaline yol açacaktır. İhlallerin önceden tespit edilememesi aynı zamanda GDPR kapsamında bildirim yükümlülüğünün yerine getirilememesi sonucunu doğuracaktır.

Olay müdahalesi için öncelikle mevcut teknik altyapının farkında ve olayları tespit etme kapasitesinin sınırları hakkında bilgi sahibi olmak gerekir. Olayları tespit etme kapasitesinin yeterli olmadığının fark edildiği noktada organizasyon, gerekli teknik altyapıyı sağlamak için harekete geçmelidir. Olayların tespit edilmesi bakımından teknik altyapı teknolojinin ilerlemesine paralel olarak yenilenmelidir. Bununla beraber, gerçekleşmiş olayların üzerinden giderek başarı ve başarısızlıklar analiz edilmeli ve bu şekilde karşılaşılabilecek olaylar için olay müdahalesi planını güncellemelidir.

Uygun bir olay müdahalesi, muhtemel senaryolar üzerinden giderek belli politikaların oluşturulmuş olması, bir derecelendirme yapılarak muhtemel olayların listelenmesi ve bu olayların meydana gelmesi durumunda ne tür iyileştirme faaliyetlerinin yapılacağının belirlenmesi ile oluşturulur. Bu şekilde uğranacak zarar minimuma indirgenmiş olacaktır.

Yukarıda sayılanların ışığında, olay müdahalesini, kişisel verilerin güvenliğini tehlikeye düşürebilecek olayları (i) tespit etmek, (ii) analiz etmek ve (iii) bu olaylara müdahale etmek olarak üç ana başlıkta toplamak mümkündür. Bu noktada esas olan tespit edilen olayın doğru bir şekilde sınıflandırılması, doğru sınıflandırmayla doğru müdahale yöntemlerinin belirlenmesi ve en kısa sürede olayın ihlal boyutuna ulaşıp ulaşmadığının değerlendirilmesidir.

Son olarak belirtmek gerekir ki, olay müdahalesi Türk Hukuku'nda karşılığını KVKK m. 12/5'te bulmaktadır. Bu madde uyarınca işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu, ihlali öğrenmesinden itibaren ilgili kişiye ve Kurum'a bildirim yapmakla yükümlü olacaktır. Ancak bu yükümlülüğü yerine getirebilmesi için veri sorumlusunun öncelikle ihlalden haberdar olması gerekmektedir.

Uygun bir olay müdahalesi planı olmadan organizasyon içindeki kişisel veri ihlallerinden önceden haberdar olmak mümkün değildir. Bu sebeple olay müdahalesi her ne kadar KVKK'da açıkça düzenlenmemiş olsa da yalnızca GDPR kapsamında bir yükümlülük olarak düşünülmemelidir. Olay müdahalesi planı olmadan KVKK m. 12/5 uyarınca bildirim yükümlülüğünün yerine getirilmesi mümkün olmayacağından olay müdahalesi aynı zamanda KVKK kapsamındaki yükümlülüklerin de bir parçası olarak düşünülmelidir.

Aydınlatma Yükümlülüğü Tebliği'nin Getirdiği Düzenlemeler

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, 10 Mart 2018 tarihinde 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Tebliğ'in düzenleniş amacı, veri sorumluları veya yetkilendirdikleri kişilerin yerine getirmesi gereken aydınlatma yükümlülüğünün tabi olacağı usul ve esasların belirlenmesidir.

KVKK m. 10 uyarınca kişisel verilerin elde edilmesi sırasında veri sorumluları, ilgili kişileri bilgilendirmekle yükümlüdür. Bu yükümlülük, veri sorumlularının veya temsilcilerinin kimliği, kişisel verilerin hangi amaçlarla işleneceği, kişisel verilerin kimlere ve hangi amaçlarla aktarılabileceği, kişisel verilerin toplama yöntemi ve hukuki sebebi ile ilgili kişinin kanundan kaynaklanan hakları konularında bilgilendirilmesini kapsar.

Tebliğ m. 5/1 uyarınca aydınlatma yükümlülüğü sözlü, yazılı, ses kaydı, çağrı merkezi, fiziksel veya elektronik yöntemlerle yerine getirilebilir. İlgili yöntemlerden herhangi biri vasıtasıyla yapılacak bilgilendirmelerde dikkat edilmesi gereken usul ve esaslar ise aynı maddenin devamında öngörülmüştür. Bu hususlar aşağıda açıklanmaktadır:

- *İlgili kişinin açık rızasına veya KVKK'daki diğer işlem şartlarına bağlı olarak kişisel verilerin işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir.*
- *Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir.*
- *Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir.*
- *Sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır.*
- *Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir.*
- *Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.*
- *Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.*
- *Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır.*
- *Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir.*
- *KVKK m. 10/1/(ç)'de yer alan "hukuki sebep"ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin KVKK m. 5 ve m. 6'da belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.*
- *Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir.*
- *Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir.*
- *Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.*

Tebliğ m. 6 ise kişisel verilerin ilgili kişiden doğrudan elde edilmemesi halinde aydınlatmanın nasıl yapılacağını düzenlemektedir. Buna göre verilerin elde edilmesini takriben makul süre içerisinde, kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişimin kurulması esnasında aydınlatma yükümlülüğü yerine getirilmelidir. Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişi aydınlatılmalıdır.

Özel Nitelikli Kişisel Veriler Nasıl İşlenmeli ve Korunmalıdır?

KVKK m. 6 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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak nitelendirmiştir. Aynı maddenin son fıkrasında özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu belirtilmiştir. Kurul bu kapsamda 31 Ocak 2018 tarihinde "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" konu başlıklı bir karar almış ve söz konusu önlemleri açıklamıştır.

Kararda özel nitelikli kişisel verilerin güvenliğine yönelik sitemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün hazırlanması öngörülmüştür. Ayrıca özel nitelikli kişisel verilerin işlenmesi süreçlerinde çalışan kişilere özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitim verilmesi, bu kişilerle gizlilik sözleşmeleri yapılması, verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin belirli olarak tanımlaması ve periyodik olarak yetki kontrollerinin gerçekleştirilmesi gerektiği belirtilmiştir. Kurul, görev değiştiren veya işten ayrılan çalışanların bu verilere erişim yetkileri bulunması durumunda, görev değişikliği veya işten ayrılma sonrasında bu alandaki yetkilerinin derhal kaldırılması gerektiğini düzenlemiştir.

Kararda özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamın elektronik veya fiziksel ortam olmasına göre alınması gereken önlemler konusunda bir ayrım yapılmıştır. Eğer veriler elektronik ortamda tutuluyorsa verilerin kriptografik yöntemler kullanılarak muhafaza edilip, bu kriptografik anahtarların güvenli ve farklı ortamlarda tutulması, verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi ve gerekli güvenlik testlerinin düzenli olarak yapılarak, bu test sonuçlarının kayıt altına alınması, verilere bir yazılım aracılığıyla erişiliyorsa bu yazılıma ait kullanıcı yetkilendirilmesinin yapılması gerekmektedir. Ayrıca verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanması yükümlülüğü getirilmiştir.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamın fiziksel bir ortam olması halinde ise yeterli güvenlik tedbirlerinin alındığından emin olunması ve fiziksel güvenliğin sağlanarak yetkisiz giriş çıkışların engellenmesi yükümlülüğü getirilmiştir.

Ayrıca bu kararda belirtilen önlemlere ek olarak Kurum'un internet sitesinde yayınlanan kişisel veri güvenliği rehberinde belirtilen uygun teknik ve idari tedbirlerin alınması gerektiği de belirtilmiştir.

Söz konusu karardan da anlaşıldığı üzere şirketlerin özel nitelikli kişisel veri işlemesi durumunda, genel bir veri işleme politikası oluşturması yeterli olmayacaktır ve özel nitelikli kişisel veriler için ayrı bir politika ve prosedürün belirlenmesi gerekecektir. Bunun yanında özel nitelikli kişisel verilerin elektronik ortamda muhafaza edilmesi durumunda birtakım teknik yatırımlar yapılması gerekecektir. Veri sorumlusunun alması gereken önlemler adına KVKK'da yer almayan birçok yükümlülüğün bu kararla getirilmiş olması sebebiyle veri sorumlularının bu kararı mutlaka incelemesi gerekmektedir.

KISALTMALAR	
ICO	Information Commissioner's Office
GDPR	General Data Protection Regulation
Kurum	Kişisel Verileri Koruma Kurumu
Kurul	Kişisel Verileri Koruma Kurulu
KVKK	Kişisel Verileri Koruma Kanunu
m.	madde
SPK	Sermaye Piyasası Kurulu

GSG Hukuk

Aylık Kişisel Verilerin Korunması Hukuku Bülteni

Nisan 2018

www.gsghukuk.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@gsghukuk.com

Nilgün Serdar Şimşek, LL.M.
Ortak, Avukat
T: +90 (212) 326 63 68
nilgun.simsek@gsghukuk.com

Rıza Eroğlu
Kıdemli Müdür
T: +90 (212) 326 64 61
riza.eroglu@gsghukuk.com

İpek Okucu Taftalı
Kıdemli Avukat
T: +90 (212) 326 60 60/3881
ipek.okucu@gsghukuk.com