Financier Worldwide - Yıllık Genel Bakış

Veri Koruma Ve Kişisel Verilere Dair Yasalar 2016*

Cüneyt Kırlar
Risk Danışmanlığı Ortağı
Deloitte Türkiye
ckirlar@deloitte.com

Sizce, bölgenizde faaliyet gösteren şirketler veri koruma ile ilgili risklere yeterince dikkat gösteriyor mu? İçinde yaşadığımız dijital çağda şirketler, gizlilik ve mahremiyet konularında üstlerine düşen görevi tam olarak anlamaya başladılar mı, ne dersiniz?

Kırlar: Kişisel Verilerin Korunmasına dair kanun Nisan 2016 tarihinde yayınlanarak, 6 ay sonraya bırakılan bazı maddeler haricinde, yürürlüğe girdi. Dolayısıyla, Ekim 2016 tarihi itibari ile yasaya uygunluğun ilk etabı tamamlanmış oldu. İlgili AB yönetmelikleri doğrultusunda hazırlanan ve "Kişisel Verilerin Korunması Kanunu" olarak bilinen yasa resmi gazetede yayınlanarak yürürlüğe girmiş olmasına rağmen, mevzuata uyum anlamında bakıldığında, firmaların olgunluk seviyesinin düşük olduğu söylenebilir. Veri mahremiyeti aslında yatırımcılar arasında ve siyasi çevrelerde uzun yıllardır konuşulan bir konu ancak birtakım sebeplerle ertelenmekteydi. Alt sektörler bazında bakıldığında, finansal hizmetler ve telekom sektörleri farkındalık ve yasaya uyum anlamında çok daha hazırlar, çünkü zaten halihazırda bu konuda çeşitli düzenlemelere tabi durumdalar ancak onların da tam uyum için atmaları gereken adımlar bulunmaktadır. İlaveten, çok uluslu şirketler ve büyük firmalar; hukuk, IT danışmanlığı ve veri koruma teknolojisi alanlarında veri mahremiyeti açısından gerekli yatırımları yapacak bütçeleri ayırmaktalar. Yürürlüğe giren yasaya dair farkındalığı artırmak ve güçlendirmek için bir Kişisel Verileri Koruma Kurumu (Kurum) kurulmasına ilişkin hazırlıklar devam etmektedir. Kurum faaliyetlerine başladıktan sonra, kişisel verilerin korunması konusuna ilginin artması beklenmektedir.

Kurumsal veri depolama, işleme ve aktarılması konusunda, bölgede faaliyet gösteren firmaları etkileyen hukuki ve düzenleyici gelişmelerden bahsedebilir misiniz?

Kırlar: Kişisel Verilerin Korunması Kanunu kişisel verilerin toplanması, işlenmesi, sorgulanması, güncellenmesi, paylaşımı ve kullanıma dair bir çerçeve getirdi. Yasa, ilgili kişinin açık rızası olmadan, kişisel verilerin işlenmesi ve yurtdışına ya da üçüncü taraflara aktarımına izin vermiyor, bunun istisnaları yasada açık ve net bir şekilde ortaya konmuş durumdadır. Yasada belirtilen haller dahilinde kullanılan verilerin de daha sonra imha edilmesi gerekmektedir. Kişisel verileri işleyen, "veri işleyeni" olarak isimlendirilen üçüncü tarafların, gerekli güvenlik seviyesini sağlayacak önlemleri alması gerekmektedir. Veriyi bulunduran ve "veri sorumlusu" olarak isimlendirilen tarafların ve işleyenlerin yasaya uyumda karşılıklı sorumlulukları bulunuyor. Veriyi bulunduran veri sorumlusu tarafın, periyodik denetimler yoluyla veri işleyicinin kişisel verilerin korunması konusunda yeterli bir seviyede olduğunu kontrol etmesi gerekmektedir. Yasadaki bir diğer önemli madde de, işlenmiş verilerin hangi ülkelere ne zaman transfer edilebileceği ve ilgili kişinin açık rızası olmayan durumlarda verilerin hangi şartlarla transfer edilebileceğini açıkça ortaya koymaktadır. Verinin transfer edileceği yabancı ülke, veri koruması konusunda yeterli seviyede olmalı hükmü bulunmakta ve yeterli seviyeyi haiz ülkelerin listesi Kurum tarafından ilan edilecektir.

Son yıllarda, veri koruma ve mahremiyet konularında izleme ve uygulama anlamında, yetkili makamların ne tür adımlar attığını ve faaliyetlerini nasıl sıkılaştırdıklarını görmekteyiz?

Kırlar: Kişisel Verilerin Korunması Kurumu, yasanın uygulanmasını takip etmekle yetkilendirilmiş durumdadır. Kişisel Verilerin Korunması Kanunu, kişisel verilerin yasaya aykırı şekillerde kullanılması halinde, 5000 TL ile 1.000.000 TL arasında idari ceza ve cezai yaptırımlar getirdi. Aydınlatma yükümlülüğü, güvenlik şartları, Kurum kararları ve veri işleme kayıt envanteri gerekliliklerine uymama halinde idari cezalar söz konusu olabilecektir. Dini inanç, vakıf, dernek ve sendika üyeliği, sağlık durumu, biyometrik, genetik ve cinsel hayata dair bilgilerin; kişinin açık rızası olmaksızın kaydedilmesi, ya da işlendikten sonra izin verilen süre içinde imha edilmemesi gibi ihlallerde, Türk Ceza Kanunu'nun ilgili maddeleri uyarınca 1 ila 4,5 yıl arasında hapis cezası getirilmektedir. Ancak Kurum'un, henüz oluşum aşamasında olması dolayısıyla cezalar uygulanabilir durumda değildir.

Son dönemlerde karşılaşılan yüksek profilli veri ihlal vakalarından nasıl dersler çıkarabiliriz? Veri koruma açısından baktığımızda söz konusu durumların etkisi ne oldu?

Kırlar: Türkiye'de veri gizliliği ihlallerine dair kamu ile paylaşılan birkaç vaka meydana gelmiştir ancak Kişisel Verilerin Korunması Kanunu'na göre, herhangi bir güvenlik ihlali durumunda, veri sorumlusu, ilgili kişiyi ve Kurum'u ivedilikle bilgilendirmek zorundadır. Kurum, söz konusu ihlali kendi web sitesi ya da uygun bulduğu başka herhangi bir yolla duyurabilmektedir. Dolayısıyla, bundan sonraki dönemde beklentimiz, veri koruması ihlallerinden doğabilecek itibar riskinin, şirket yönetim kurulları için yüksek öncelikli gündem haline gelmesi olacaktır. Son dönemde yaşanan vakalar, veri ihlali söz konusu olduğunda bunu kısa sürede belirleyebilmenin, herhangi bir anomali ya da ihlali hızlıca teşhis

edebilecek yetkinlikleri geliştirmenin muhtemel saldırılar ile mücadelede hayati önemi olduğunu göstermektedir.

Danışman, bayi ya da distribütör gibi üçüncü taraflarla çalışılması, firmayı veri koruma anlamında bir takım özel risklere maruz bırakabiliyor. Bu riskler nelerdir ve bu risklere karşı nasıl önlemler alınabilir?
Kırlar: Üçüncü taraf kullanımı bugün iş dünyası değer zincirinin ayrılmaz bir parçasıdır ve üçüncü şahıs riski firma tarafından çok hassas bir şekilde yönetilmelidir. BDDK bankacılık sektöründeki destek hizmetleri kullanımını düzenlemiştir ve bankacılık sektörünün uyması gereken kontrol çerçevesini belirlemiştir. Diğer sektörler için ise böyle bir düzenleme bulunmamaktadır. Kişisel verilerin korunmasına dair yürürlüğe giren kanun, kişisel verilerin üçüncü taraflara aktarımına dair şartları ve kişisel veri işleyenlerin sorumluluklarını ortaya koymaktadır. Sözleşme yönetimi üçüncü taraf riskinin etkin yönetimi için hayati önem taşımaktadır. Ek olarak, yasa ile belirlenen güvenlik kontrollerinin uygulamaya konduğundan emin olunması için, sözleşmelerdeki gizlilik maddesi, veri koruma sorumluluklarının üçüncü taraflara aktarımı konusunu da içerecek şekilde yapılandırılmalıdır.

Kurum içi veri mahremiyeti risk ve tehditlerinin yönetimi anlamında, örneğin kayıp cihazlar ya da yanlış hareketlerde bulunan çalışanlar söz konusu olduğunda, firmalar doğabilecek yükümlülüklere karşı neler yapabilirler?
Kırlar: İnsan faktörü, risk yönetiminin ayrılmaz bir parçasıdır ve ek olarak, veri koruma konusunda çalışan farkındalığını arttırmaya yönelik ihlallerle mücadelede büyük önem taşımaktadır. Çalışanlar, yeni Kişisel Verilerin Korunması Kanunu ile kendilerine tanınan hak ve yüklenen sorumluluklardan net bir şekilde haberdar edilmelidir. Gizlilik sözleşmeleri ve çalışanların kontratlarında mahremiyet ile ilgili maddeler olmalı, firma cihazları, yazılım ve verilerinin kullanım şartları açık ve net bir şekilde belirtilmelidir. Çalışan eğitimlerine ek olarak, firmalar şahsa özel verilerin sızdırılmasını önlemek maksadıyla, otomatik kontrol sistemlerini devreye almalıdır. Veri envanteri oluşturulduktan sonra, firma hangi verilerin korunması gerektiğine ve erişim kontrolü, şifreleme ve veri sızdırılmasının önlenmesi maksadıyla hangi teknik çözümlerin uygulamaya konulacağına sağlıklı bir şekilde karar verebilir. Disk şifreleme metodu firma cihazlarında yaşanabilecek kayıp ve çalıntı durumlarında firma verilerinin korunmasını sağlayan temel yöntemlerden biridir.

Bölgenizde faaliyet gösteren firmalara, veri risk yönetimi, mevzuata uyum iç süreçlerinin tesisi ve veri mahremiyeti mevzuatına uyum konularında, ileriye dönük olarak hangi tavsiyelerde bulunursunuz?
Kırlar: Kişisel Verilerin Korunması Kanunu'na uyum şu anda Türkiye'de faaliyet gösteren şirketler için sıcak gündem maddesidir. Mevzuata uyum seviyesinin arzu edilenin altında olduğunu ancak firmaların birtakım yol haritaları oluşturarak ederek, süreç, teknoloji ve insan gücüne yatırım yapmak yoluyla farkı kapatmaya çalıştıklarını görmekteyiz. Yeni alt mevzuatlar hazırlık aşamasındadır ve bunlar yürürlüğe girdiğinde şu anda muğlak gibi görülen konular biraz daha netlik kazanacaktır. Firmaların kişisel veri envanterlerini tanımlaması, ana veri akışlarını çizmesi, temel riskleri belirlemesi ve bunlara göre de gerek otomasyonlu gerek manuel kontrol sistemleri kurarak veriyi güvenceye alması

gerekmektedir. İç denetim bölümleri yıllık iç denetim planlarında kişisel verilere ilişkin kontrolleri de denetim sürecinin bir parçası olarak ele almalı ve firmanın, Kişisel Verilerin Korunması Kanunu'na uyumu konusunda yönetim kuruluna güvence verebilmelidir. Veri koruma alanında sürdürülebilir bir uyum programının oluşturulması için, mahremiyet temelli bir tasarım anlayışı benimsenmeli, mahremiyet konusu proaktif bir şekilde tasarım, IT sistem işleyişi, altyapı network ve genel iş uygulamalarına entegre bir şekilde çerçevelendirilmelidir.

**Röportaj, Financier Worldwide dergisinin, Aralık 2016 tarihli, Yıllık Bakış 2016 sayısında yayımlanmıştır.*