ÖZEL NİTELİKLİ VERİLERİN İŞLENMESİNDE VERİ SORUMLULARINCA ALINMASI GEREKEN ÖNLEMLERE İLİŞKİN 2018/10 SAYILI KURUM KARARI HAKKINDA BİLGİ NOTU

Kişisel Verilerin Korunması Kurumu ("Kurum") tarafından 30356 sayı ve 10 Mart 2018 tarihli Resmi Gazete'de yayımlanan 2018/10 sayılı karar ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("Kanun") tanımlanmış olan özel nitelikli kişisel verilerin işlenmesi sırasında veri sorumluları tarafından alınması gereken idari ve teknik önlemler Kanun'un 6/4 maddesinin Kurum'a verdiği yetki kapsamında belirlenmiştir. Söz konusu kararda:

1- Veri sorumlularının özel nitelikli kişisel verilerin güvenliğine ilişkin ayrı bir politika ve prosedür belirlemesi gerektiği,
2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde görev alan çalışanların; a) düzenli eğitimlere tabi tutulması, b) görevlerine ilişkin gizlilik sözleşmelerinin yapılması, c) verilere erişim yetkisine sahip kişilerin yetki kapsamlarının ve sürelerinin net olarak belirlenmesi, ç) periyodik yetki kontrollerinin gerçekleştirilmesi, d) görev değişikliği olan veya işten ayrılan çalışanların yetkilerinin derhal kaldırılması ve bunlara verilen veri envanterlerinin geri alınması gerektiği,
3- Şayet özel nitelikli veriler elektronik ortamda tutuluyorsa; a) verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi, b) kriptografik anahtarların güvenli ve farklı ortamlarda tutulması, c) veriler üzerinde gerçekleştirilen tüm hareketlerin kayıtlarının güvenli olarak loglanması, ç) verilerin bulunduğu elektronik ortama ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması ve test sonuçlarının kayıt altına alınması, d) verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması ve test sonuçlarının kayıt altına alınması, e) verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin kurulması gerektiği,
4- Şayet özel nitelikli veriler fiziksel ortamda tutuluyorsa; a) söz konusu ortamın elektrik kaçağı, yangın, su baskını, hırsızlık gibi risklere karşı yeterli güvenlik önlemlerinin alınması, b) ortama yetkisiz giriş ve çıkışların önlenmesi için güvenlik önlemlerinin alınması gerektiği,
5- Özel nitelikli kişisel verilerin aktarımı söz konusu olacaksa; a) verilerin e-posta yoluyla aktarımında kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılması, b) taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarım yapılacaksa bunların kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması, c) farklı fiziki ortamlardaki sunucular arasında aktarımlarda VPN veya sFTP yöntemiyle veri aktarımı yapılması, d) kağıt ortamında aktarımlarda evrakın çalınması, kaybolması ya da yetkisiz kişilerce görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın gizlilik dereceli olarak işaretlenmesi gerektiği,
6- Kurum tarafından yayımlanmış olan Kişisel Veri Güvenliği Rehberi'nde yer alan diğer teknik ve idari tedbirlerin alınması gerektiği,

kararlaştırılmıştır.

Legal Hukuk Bürosu