Konu : 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuatına uyum hakkında bilgilendirme.

Sayın YYYşirketi,

Bildiğiniz üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun" veya "KVKK") 7 Nisan 2016 tarihinde Resmi Gazete'de yayınlanmak suretiyle yürürlüğe girmiştir. Kanun gereği kişisel veri işleme süreçlerini yürüten ve Kanun'da sayılan şartları taşıyan veri sorumluları ve veri işleyenlerin birtakım yükümlülükleri bulunmaktadır.

XXX Şirketi olarak temel insan haklarından biri olması sebebiyle kişisel verilere atfettiğimiz önem bir hayli fazladır. Bu sebeple Kanun ve ilgili mevzuatına uyum için gerekli süreçler Şirketimizce yürütülerek Kanun'a uyum sağlanmıştır.

Yine bildiğiniz üzere Kanun gereğince veri sorumlusu, *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"yi;* veri işleyen ise, *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"yi* ifade etmektedir.

Kanun'un 12. maddesinin 2. fıkrası gereğince *"Veri sorumlusu kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur."*

Aynı maddenin 4 numaralı fıkrası ise *"Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder."* Hükmünü havidir.

Bu sebeple Şirketimiz adına veri işleme faaliyeti yürüten ve Kanun gereği veri işleyen tanımına dâhil olduğunuzu hatırlatmak isteriz. Kanun'a uyum sürecinde Şirket olarak üzerimize düşen tüm yükümlülükleri tam ve eksiksiz olarak yerine getirmek için azami çaba sarf etmekteyiz ve veri işleyenlerimiz olarak sizlerin de bu çabayı göstermeniz hem kanuni hem sözleşmesel bir yükümlülüktür. Bu çerçevede Şirket olarak kişisel veri ihlallerinin önüne geçebilmek ve bir ihlal durumunda zararı en aza indirebilmek için tarafımızca alınan ve veri işleme faaliyetlerinizin türüne göre değişebilecek olmakla beraber asgari olarak sizden de beklediğimiz idari ve teknik tedbirler şunlardır:

İdari Tedbirler

- Şirket bünyesinde bilgi güvenliği yönetim sisteminin kurulması ve işletilmesi,
- Şirket personelleri ve ilgili taraflar ile taahhütnameler ve gizlilik sözleşmelerinin imzalanması,
- İş süreçleri üzerinde risk analizlerinin gerçekleştirilmesi,
- Kişisel veri envanterlerinin oluşturulması,
- Bilgi güvenliği politika ve prosedürlerinin işletilmesi,
- Bilgi güvenliği ve kişisel veri işleme faaliyetleri hakkında eğitimlerin düzenlenmesi ve değerlendirilmesi,

- Çalışan bilgisayar vb. araç gereçlerine yetkisiz erişimlerin önüne geçmek adına söz konusu araç ve gereçleri yalnızca yetkili kişilerin kullanması,
- Şirket içi ya da bağımsız denetimler ile faaliyetlerin gözden geçirilmesi,
- Yapılan işlemler için objektif delil üretecek kayıtların oluşturulması,

Teknik Tedbirler

- Sızma testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Sistemler üzerinde yazılımsal değişiklik ve/veya güncelleme yapılacağı zaman denemeler test ortamında yapılmakta, varsa güvenlik açıkları tespit edilerek gerekli tedbirler alınmakta ve yapılacak değişikliğe son hali bu işlemlerin ardından verilmektedir. (Kararda geçiyor, yapılması gerekli.)
- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlerle ilgili teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun hazırlık çalışmaları yapılmıştır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir. (Altına ayrıca yazılacak)
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır.
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.
- Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

Burada gösterilenler ve/veya kendi veri işleme süreçlerinize göre belirlemiş olduğunuz tedbirleri almanızın yanı sıra, veri sorumlusu olarak bünyemizde gerçekleşebilecek bir ihlal durumunda veya bir ilgili kişinin başvurusuna cevap verebilmek adına tarafınızla da irtibata geçilebilecektir. Böyle bir durumda veri işleyenimiz olarak azami dikkat ve özeni göstererek

gerekli iş ve işlemleri gerçekleştirmeniz, konu hakkında ilgili tarafları ve Şirketimizi bilgilendirmeniz büyük önem taşımaktadır.

Tüm bu sebeplerle Kanun ve ilgili mevzuatına hem kendi veri işleme süreçleriniz açısından veri sorumlusu olarak, hem veri işleyen sıfatı ile azami özen göstermeniz ve işleme süreçlerinizi Kanun'a uyumlu hale getirmeniz gerekmektedir.

Gereğinin yapılması hususunu önemle hatırlatırız.