

KVKK UYUM SÜRECİ EĞİTİMİ

Leyla KESER

5.9.2016

- **MEVCUT DURUMUN TESPİTİ**
- Şirketin her bir departmanı itibariyle;
 - Kişisel veri akış kaynaklarının tespiti
 - Web sitesi
 - Çalışan
 - Müşteri
 - Çağrı merkezinden
 - Uygulama yazılımlarından
 - Form doldurarak ıslak imzalı

- Tedarikçiler
 - Gerçek kişi tacir
 - Tüzel kişi tacir
- Ziyaretçiler
 - Fiziksel olarak binalara giriş yapan kişiler
 - » Çalışan
 - » Diğer ziyaretçiler
- İnternet sitesi ziyaretçileri
- Yurt İçi ve/veya yurt dışında yerleşik şirketlerle/İştiraklerle Veri Aktarımı yoluyla alınan veriler

ANALİZ AŞAMASI

- Departmanlardan gelecek bu bilgiler doğrultusunda:
 - Şirketin kişisel veri haritasını çıkarmak
 - Kişisel verinin yaşam döngüsünü tespit etmek

- İşlediği kişisel veri çeşitlerinin,
- Kişisel veriyi işleme amaçlarının,
- Kişisel veri işleme ilkelerinin,
- Kişisel veriyi işleme dayanaklarının,
- Kişisel veri saklama sürelerinin,
- Kişisel veriyi silme, yok etme veya anonimleştirme yöntemlerinin,
- Kişisel veriye erişim yetki ve kısıtlamalarının,
- Kişisel veriyi aktardıkları yurt içi/yurt dışı üçüncü kişilerin tespiti.
- Şirketin Kişisel veriyi;
 - Muhafaza etmek
 - Hukuka aykırı işlenmesini engellemek,
 - Yetkisiz erişimlere karşı korunmasını sağlamak amacıyla aldığı teknik ve idari tedbirlerin neler olduğunun belirlenmesi.

– KVKK UYUMU

- Kişisel verileri işleyen tarafla yapılacak sözleşmede;
 - Veri işleyenin de bu güvenlik önlemlerinin alınması noktasında veri sorumlusu ile müştereken sorumlu olduklarının belirtilmesi,
 - Veri işleyen ve veri sorumlularının süresiz olarak sır saklamakla yükümlü olduklarının sözleşmeye dahil edilmesi,
 - Veri ihlali yaşandığında, veri sorumlusunun bu durumu derhal ilgili kişiye ve Kurul'a bildirmesini sağlayacak süreç tasarımı,
 - Uhdesinde olan yükümlülöklere uyumun sözleşmede öngörölecek bir denetim mekanizması ile kontrolünün sağlanması gereklidir.

- Kurumsal politika ve prosedürlerin yeniden gözden geçirilmesi
 - Kişisel verilerin korunması politika belgesi
 - İnternet kullanımı politika belgesi
 - E-mail kullanımı politika belgesi
 - Bilgisayar/cep telefonu kullanımı politika belgesi
 - Kayıt yönetimi politika belgesi

- İşlenen kişisel verinin niteliği ve Şirket açısından önemine göre;
 - Şifreleme, sFTP, hash, vpn kullanımı gibi teknolojilerin devreye sokulması,
 - Privacy by design ve Privacy Enhancing Technologies (PETs) kullanımı (DLP gibi),
 - Kişisel veriye erişim açısından;
 - Her bir departmanın organizasyon şeması çıkartılarak; erişim hususunda roller, görevler, sorumluluk ve yetki ayrımlarının belirlenmesi,
 - ID yönetimi
 - Bilişim sistemlerinin bu erişim kısıtlaması veya yönetimi şemasına göre konfigürasyonun sağlanması,
 - Şirket içi yetkisiz erişimi önleyecek teknolojiler veya uygulamaların devreye alınması.

- Mahremiyet Risk değerlendirme/Varlık değerlendirme
- Aydınlatma metni
- İlgili kişinin kişisel verileri üzerinde haklarını kullanacağı süreçler
- İnternet sitelerindeki gizlilik ve kişisel verilerin korunması ilkeleri
- Sözleşmelerde yer alan gizlilik ve kişisel verilerin korunması klozları

- Çalışanların;
 - Kişisel verilerinin işlenmesi bakımından açık rızalarının alınması
 - Rıza alınması kuralının istisnalarının değerlendirilmesi
 - İş akitlerinin kişisel verilerin korunması ve açık rızaya ilişkin olarak güncellenmesi
 - İş akitlerinin kişisel verilere ilişkin olarak süresiz olacak şekilde sır saklama yükümlülüğünü ihtiva edecek şekilde değiştirilmesi.

- Müşterilerin;
 - Açık rızalarının alınması
 - Rıza alınması kuralının istisnaları
- Yurt içi veya yurt dışında mukim 3. Kişilerle yapılan kişisel veri aktarımı öngören her sözleşmenin revize edilmesi veya ek protokoller düzenlenmesi
- NDA'lerin revize edilmesi
- İç/Dış denetim öngörülmesi

- Veri Sorumluları Siciline kayıt yükümlülüğü (7 Ekim 2016 tarihinde Kurul oluştuktan sonra ilan edecek)
 - a) Veri sorumlusu ve **varsa temsilcisinin** kimlik ve adres bilgileri.
 - b) Kişisel verilerin hangi amaçla işleneceği.
 - c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.
 - ç) Kişisel verilerin aktarılabilceği alıcı veya alıcı grupları.
 - d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.
 - e) Kişisel veri güvenliğine ilişkin alınan tedbirler.
 - f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.
- Veri Sorumlusu temsilcisi?

- **Suçlar**

- MADDE 17- (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.
- (2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

- **Kabahatler**
- MADDE 18- (1) Bu Kanunun;
 - a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
 - b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
 - c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
 - ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir.
- (2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

- **İstisnalar**
- **MADDE 28-** (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:
- a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.
- **b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.**
- c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.
- **d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.**

- (2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:
- a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- **b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.**
- c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

- **Yönetmelik**
- **MADDE 31-** (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur.

- **Geçiş hükümleri**
- **GEÇİCİ MADDE 1-** (1) Bu Kanunun **yayımlı tarihinden itibaren altı ay içinde** 21 inci maddede öngörülen usule göre **Kurul üyeleri seçilir ve Başkanlık teşkilatı oluşturulur.**
- (2) **Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.**
- (3) Bu **Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler**, yayımı tarihinden itibaren **iki yıl içinde** bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu **Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir.**
- (4) Bu Kanunda öngörülen yönetmelikler bu **Kanunun yayımı tarihinden itibaren bir yıl içinde** yürürlüğe konulur.
- (5) Bu Kanunun yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir.

- **Yürürlük**
- **MADDE 32-** (1) Bu Kanunun;
- a) 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri **yayımlı tarihinden altı ay sonra,**
- b) Diğer maddeleri ise **yayımlı tarihinde,**
- yürürlüğe girer.

- Çok teşekkür ediyorum
- leyla.keser@gmail.com