KİŞİSEL VERİLERİN KORUNMASI KANUNUNUN GETİRDİKLERİ

Yıllardır bilgi güvenliği camiasında ha çıktı ha çıkacak denilen kanun tasarısı nihayet 6698 Kanun numarası ile yasalaştı.

Ancak bu devrim niteliğinde olayın kamuoyunda yeterince ilgi uyandırmadığını düşünüyorum. Vatandaşı korumaya yönelik olan bu kanun, vatandaşa pek çok hak, kişisel veriyi kullanan ya da bulunduran kurumlara ise çok fazla yükümlülük getirmekte.

Aslında bilgi güvenliği yöneticilerinin, danışmanlarının ve denetçilerinin elini sağlamlaştıracak bu kanun, diğer yandan, getirdiği yükümlülüklerin ağırlığına ve uyum için tanınan süreye bakıldığında kuruluşlar açısından epey bir zorluk yaratacak gibi görünüyor.

Tanınan süre sonunda uyumun sağlanamaması ve oluşacak şikayetler, kurum tarafında ciddi yaptırımlara neden olacak. Kanunun herhangi bir maddesinin ihlali para cezasının yanı sıra icra kurulundaki yöneticilerin 1 – 3 yıl hapis cezası ile cezalandırılmasına neden olabilecek. İhlal konusu verilerin, sağlık, etnik köken, din, cinsel, parti ya da dernek üyeliği gibi özel bilgiler kapsamındaki verilerden olması halinde bu ceza 1.5 katına çıkarılacak.

Peki kişisel verinin tanımı nedir? Hangi veriler kişisel veri olarak ele alınıyor? Tek bir bireyi işaret edebilecek her türlü veri kişisel veri sayılıyor. Yıllarca kurumlarda hep tartışılıp genellikle pek de bir sonuca varılamamıştır; örneğin cep telefonu numarası tek başına ise bir kişisel veri midir? Bu veriden yola çıkarak, o telefonu kullanan ya da yasal sahibi olan kişiye ulaşabileceğimiz için, evet kişisel veridir. Bu durum hayatımızı oldukça zorlaştıracak gibi görünüyor, değil mi ?

Vatandaş olarak bakarsak, bundan sonra kişisel olarak istediğimiz kuruma dilekçe vererek, kişisel verilerimizin bu kurumda saklanıp saklanmadığını, saklanıyorsa nedenini, saklanmasını istemiyorsak da silinmesini talep etme hakkımız var. Kurumun da bu dilekçeyi aldıktan sonra 30 gün içinde vatandaşa cevap verme zorunluluğu bulunuyor.

Bu kanuna uyum için tanınan süre, yeni veriler için 6 ay, eldeki mevcut tüm verileri de uyumlu hale çevirebilmek içinse 1 yıl.

Kanunun Resmi Gazetede yayınlanma tarihi 07 Nisan 2016 olduğuna göre 1 ay çoktan geçmiş bile. Bu yazının yayınlandığı tarihten yaklaşık 5 ay sonra yani 6 Ekim 2016'da vatandaş tarafından kurumunuza verilebilecek bu tür dilekçelere cevap verebilir durumda olmanız gerekiyor.

Peki acaba kurumların hazırlıkları nasıl gidiyor? Bu kalan kısa sürede neler yapılması gerekiyor?

1- Öncelikle veri envanterinizi oluşturun.

2- Saklayacağınız, işleyeceğiniz, transfer edeceğiniz kişisel veriler için açık rızanın nasıl alınacağını kurgulayın. Transfer kavramı, verinin kurum dışına çıkarıldığı her türden durumu kapsıyor. Buna aynı grup içindeki kardeş şirketler de dahil.

3- Elde tutulan kişisel verilerin tutulma amaçlarını net olarak belirleyin. Bu amaç çok net değilse, ya da iş ihtiyacı kalmadıysa veri daha fazla elde tutulamaz.

4- Saklanan kişisel verilere bir kullanım ömrü belirlenmeli. Artık bu veriler sonsuza kadar tutulamayacak. Ya da kuruluş, bir kere veriyi edindi mi dilediği kadar ve dilediği maksatla kullanamayacak.

5- Kurumunuz içinden kıdemli bir çalışanı veri sorumlusu olarak tayin edin. (Dikkat: bu çalışanınız herhangi birisi olmamalı, gerçekten kurumunuzda bu kanunun gerekliliklerinin yerine getirilmesini sağlayabilecek, süreçlere hakim, yaptırım gücü olan birinin olması gerekiyor. Kötü haberse, herhangi bir ihlal durumunda yöneticilerle birlikte bu arkadaş ta ceza alabilecek)

6- Bütün bu çalışmalarınız, elinizdeki kişisel verilerin envanteri, elde tutulma amacı, saklama süresi, kimlerle paylaşıldığı, paylaşılma amacı ve veri sorumlunuzun sicili Kişisel Verileri Koruma Kurumu'na sunulacak. Kişisel Verileri Koruma Kurumu Başbakanlık bünyesinde kurulmuş olan resmi bir kurumdur.

Bu kanunun temelinde, verinin her türlü kullanımı ve saklanması durumları için kişiden açık rıza alınması şartı olduğu görülmekte. Yani, veri, izinsiz şekilde bir yerden alıp kurum dışındaki herhangi bir yere hiçbir şekilde transfer edilemeyecek ya da kullanılamayacak. Veri hiçbir şekilde işlenemeyecek. Veri işlemekten kasıt ne olabilir? Kanun bunu açıkça tanımlamış; veri üzerinde gerçekleştirilebilen her türlü işlem!

Yani kısacası artık hiçbir şey eskisi gibi olmayacak. Kurumlar artık ellerindeki kişisel verilerin sahibi değiller, en masumundan, örneğin herhangi bir iş ortaklığı, kampanya, araştırma vb nedenlerle bu verileri herhangi bir 3.tarafa gönderemeyecekler. Her türlü işlem için veri sahibinin açık rızası gerekiyor.

Açık rıza ne demek olabilir? Açık rıza, açıkça görülebilen, gerçekten veri sahibinden alındığını kanıtlayabildiğimiz her türlü onay. Bunun için örneğin sözleşmelere hangi verilerin ne maksatla alındığı, kimlerle paylaşılacağı, ne kadar süre elde tutulacağı bilgisi açıkça eklenebilir.

Kanun bu kadar zorlayıcı olmakla birlikte şöyle bir kolaylık da getiriyor; kişisel veriler, anonimleştirilmeleri halinde, izin alınmadan,kullanılabilecek. Anonimleştirme, veriyi, kişiyi tespit edemeyeceğimiz şekle dönüştürmek şeklinde tanımlanabilir. Örneğin; 25-35 yaş aralığında İstanbul'da yaşayan ve ücretli bir erkek çalışan.

Görüldüğü gibi kanunun gereklilikleri ve yaptırımları çok ağır, geçiş süresi ise çok kısa. Bireylere vermiş olduğu haklar ise kurumları zorlayacak nitelikte. Kamuoyunda bunun bilinirliğinin artması ile birlikte, hazırlıksız kurumlar bu durumdan kötü etkilenebilirler.

Bu nedenle kişisel veri ile çalışan kurumlar artık ellerindeki kişisel veriyi kendi mülkiyetlerindeki bir varlıkmış gibi görmekten vazgeçip, bu verilerin sadece emanetçisi olduklarını anlamalı ve veri koruma politikalarını buna göre oluşturmalılar.

Kanuna uyum için gerekli çalışmalara da en hızlı şekilde başlamalılar ki bu durumda bile gerekli hazırlıkların geçiş süresi içinde tamamlanması kolay görünmüyor.

Yeşim ÜREL

Bilgi Güvenliği ve İş Sürekliliği Danışmanı, Denetçisi

CISA, ISO 27001 LA, ISO 22301 LA