

Veri İhlalinde Alınması Gereken Aksiyonlar Nelerdir?

KVKK 2019/10 sayılı karar ile, veri ihlal bildirimlerine dair bildirim süresi, yönetimi ve yapılması gerekenler gibi önemli bazı hususlara açıklık getirilmiştir. Bu kapsam doğrultusunda;

KVKK kapsamında veri ihlalden önce hazırlanmış olması beklenen “Veri ihlali müdahale planı”nda belirtilen kişilere veri sorumlularının raporlama yapması ve ihlalden sorumlu kişilerin belirlenmesi gerekmektedir.

İhlal gerçekleşme tarih/saatini, kaynağını, etkilenen kişi ve grupları, tahmini kişi ve kayıt sayısını yani durum tespiti yapması gerekir. Bu tespitten sonra en geç 72 saat içinde Kurul’a bildirmeleri gerekir.

Veri sorumluları, ihlalin olası sonuçlarını risk ve etki analizi yaparak hem organizasyon hem de ilgili kişiler için değerlendirmeleri gerekir.

Bu adıma kadar yapılan aksiyonların ve bu adımdan sonra yapılacak aksiyonların belgelendirilmesi ve kronolojik kayıt tutulması gerekir.

Veri sorumlularının ihlale dair takip işlemlerinin yapması ve herhangi bir güncelleme olduğunda ilgili bütün kişi, kurum ve kuruluşları bilgilendirmelidir.

Risk ve etki analiz sonuçlarını göz önünde bulundurarak silinmiş, kaybolmuş verilerin geri kazandırılması veya kurtarılması için iyileştirme çabalarının olması ve bunun süresinde dair tahminlerin yapılması ve veri ihlal bildirim formunda bulundurulması gerekmektedir.

Veri sorumlularının, eğer Kurul dışında ilgili organizasyon ve/veya resmi kuruluşlar varsa ilgili sözleşmelere veya yükümlülüklerle dayanarak bildirim yapılması ve aksiyon alınması gerekmektedir.

Benzer şekilde, eğer gerekiyorsa yabancı veri otoritelerine bildirim yapılması gerekip gerekmediği belirlenerek veri sorumlularınca aksiyon alınması gerekmektedir.

Veri ihlaline sebep olan konular hakkında gerekli tedbirlerin alınıp risklerin minimize edilmesi gerekmektedir.

Bu noktaya kadar KVKK kapsamında korunması gereken veriler için ihlal sonrası gerekli adımların gerçekleştirilip gerçekleştirilmediği kontrol edilmelidir. Eğer tamamlanmadıysa ivedilikle tamamlanmalıdır.

Yukarıdaki adımlar bağlamında doğan sonuçlarla birlikte;

- Kanun’un 12. maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar
- Kanun’un 15. maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilebileceğini unutmamak gerekir.

Kaynakça

<https://www.ozbek.av.tr/kvk-blog/kisisel-verileri-koruma-kurulu-nun-kisisel-veri-ihlali-bildirim-usul-ve-esaslarina-iliskin-karari/>

<https://www.ozgunlaw.com/makaleler/kisisel-veri-ihlalleri-ve-ihlal-bildirimi-831>